MOPAC | MAYOR OF LONDON
OFFICE FOR POLICING AND CRIME

METROPOLITAN POLICE

MOPAC MPS Oversight Board
21 April 2022

Information Governance

Report by: MPS Director of Data, Aimee Reed

---

1. Purpose of this Paper

This paper describes MPS progress on information governance from April 2021 to March 2022.

2. Recommendations – that the Oversight Board:

a) Note the MPS transformation in information governance over the last three years
b) Recognise that the MPS has built strong data foundations in the last year (2021/22) that have also improved its reputation, breadth and influence nationally
c) Acknowledge the six challenges to further maturing our information governance (Section 6)

3. Executive Summary

- Over the last three years the MPS has seen a transformation in its approach to, and delivery of, information governance.
- The MPS has laid strong data foundations upon which it can accelerate work in analytics and data science in 2022/23
- Independent assessment by the Information Commissioner's Office assures the frameworks we have in place to govern our processing of data, and our management of information risk, in a lawful way.
- The MPS are well respected across law enforcement for our strategic approach to Digital, Data, Analytics and Technology (DDAT). We lead numerous national portfolios and have a place at many Home Office and cross-government forums as a result.
- Significant progress has been made on all five information governance commitments made in last year's Oversight Board report. These include;

- **Improving accessibility of data** to the frontline, analysts and senior decision makers, through a **data portal** and **raising data literacy** through simple “how to” videos to improve awareness of information governance at the point of action (such as data sharing or responding to a member of the publics information request)
- Enabling **better use of the data** we hold through improving data **quality** and streamlining data **sharing** with pan-London partners.
- Introducing **core technology** for information governance, especially the completion of an **Evidential Data Archive** so we can lawfully review, retain and dispose of data before we go live with Connect, Command & Control and BSS. We continue to lead the way on **Facial Recognition** and have consolidated some of our technology needs for data processing and privacy rights.
- Maturing our **analytics and data science skills** and operating environment through pan-MPS analytics apprenticeships and specialist machines.
- Consolidating our governance and accountability for data and having this assured independently. We recognise that the project to enable us to review and appropriately retain or dispose of data is critical to our progression as a data-driven organisation; we still have to focus investment and resources on records management

- We have six challenges to our continued progression in 2022/23. These include;
  - recruiting, retaining and developing the right **DDAT skills**
  - reviewing our **enterprise architecture** and reducing the information governance risk from new technologies and the **grey estate**
  - **aligning data and digital governance**
  - Strengthening our **data literacy** and skills across the MPS, especially for Information Asset Owners, DDAT professionals and the frontline who are critical to **data quality** at the point of entry and using the data better to drive decision-making
  - Shifting our organisational mind set to embrace an **Open Data Strategy** as it will bring a wealth of benefits for transparency, trust, engagement, data-sharing and reducing demand for privacy rights.
  - Adapting to changes anticipated in **data legislation reform**. MPS and Counter Terrorism Policing have been instrumental in influencing significant changes that will be before Parliament in the summer, however, the outcome will require considerable work to update our operating policies, procedures and training.

4. Full Report - Context

4.1. **Year on year improvements:** During 2018/19 a small group of information assurance professionals supported the Senior Information Risk Owner (SIRO) to oversee all MPS information risks. These arrangements were woefully inadequate and by 2019 the MPS was subject to numerous Enforcement Notices, an adverse Supreme Court judgement on the retention of data and an impending IPCO review. The ICO described the MPS as the most complained about organisation in the UK on public privacy rights.

4.2. In 2019 Oversight Board sought assurance that MPS information governance would significantly improve. Investment and strategic commitment from the Commissioner and Portfolio Investment Board signalled a step-change in recognition of the criticality of Digital, Data, Analytics and Technology (DDAT) to Policing priorities.

4.3. The MPS began 2020 “fire-fighting” pre-existing data risks while taking stock of existing governance, creating the foundation for progress through 2021; reviewing how our data was lawfully processed and used by the business; establishing governance, understanding data holdings and training staff on data safety.

4.4. **Progress in the last twelve months** - This year’s report illustrates the transformation made since 2019, made possible by determined effort on structures “below the surface”. It is not headline grabbing work, but positions the MPS to deliver on our ambition to optimise benefits from analytics, AI and open data to maximise data exploitation for the front line. (See **Appendix A** for a summary of progress since 2019).

4.5. **Consolidating our National Position:** It is worth noting that alongside MPS-wide improvements in 2021/22 we have also successfully increased our reach and influence into Data, Digital, Analytics and Technology (DDAT) across the sector. The MPS now occupies an incredibly strong position across the National Police Chiefs Council (including Chairs for the National Police Technology Board, National Policing Data Board and Biometrics; Facial Recognition Board). Reach into the Home Office and wider cross-government partnerships has also strengthened through working groups on algorithmic transparency and data ethics, alongside influencing and decision making positions on Home Office Data & Information Board, Strategic Capabilities Investment Board and Data Legislation Reform Steering Group.

5. Developments and successes since last Oversight Board

5.1. The commitments signalled as priorities for 2021 focused on laying the foundations for good data governance. We know that this will unlock opportunities for data science and analytics across the MPS. These were;

- Improving data **access** - working with more operational teams to safely drive value from data and maturing **data literacy**
- Being better with data – data **quality,** data **sharing**, data **ethics**, including an **Open Data Strategy** (i.e. greater transparency and openness of our data to the public and our partners),

- Investing in **technology** to improve our lawful and ethical retention of data and the processing of that by officers and staff.
- Expansion of analytics and **the profession of analysis & data science**
- Volunteering for an ICO Audit in autumn 2021 to review our **compliance and delivery against DPA (2018)**; checking progress on our information governance.

5.2. **Progress has been made in all these areas**. This is outlined in the sections below, in some cases this has been leading edge for the policing sector. We now have a consolidated set of data foundations upon which to accelerate our work in 2022/23 to seize the opportunities provided by DDAT to serve the public and improve our performance.

5.3. **Commitment One - Data Accessibility & Improved Literacy** – This year we have put more data in the hands of operational officers and staff than ever before. We haven't just done this "at scale" but have concurrently developed a "one stop shop" that makes data available to them. Whilst we are not yet at the stage of a single system that enables self-service to all data, we have consolidated what was already available and simultaneously introduced new services with simple "how to…" guides to support usage. Critically, from a data governance perspective, development is managed by experts (data engineers) centrally, 'privacy by default' principles of the DPA (2018) are built into all tools.

5.4. Whilst the full range of services now available are too numerous to list here, examples of note include web-based interface for geocoded crime data, saving hours of time for officers and staff, broadening access to self-service reporting tools (Met Insights and MetStats2) and redeveloping all our operational dashboards to be DPA complaint and, most importantly, built with users (dashboard use by the front-line is up 25% on last year as a result) see **Appendix B** for more detail on these

5.5. To complement our **increased accessibility** we have commenced our work on **data literacy.** This year has focused on "getting the basics right" and raising awareness of how to use data safely and securely. We focused a series of short, simple videos[1] (that are for watching at-the-point-of-action) to improve timeliness of responses by officers and staff to FOI and SAR requests, data sharing and information security. A monthly series of intranet articles and blogs about cyber and information security have also focused on improving the reporting times, and prevention, of data breaches and keeping information secure. Completion of our mandatory training for Data Protection (Information & You) has a very high completion rate (approx. 90%). We see considerable risk in the conversely low completion rates of this training by our external/3rd party users

5.6. Our work to conduct a learning needs analysis on data literacy for the whole MPS, and ultimately build curriculum content for our data literacy programme, has not progressed as quickly as we would have liked. Largely this is the lack of an appropriate provider in the market – policing is very niche and the knowledge of the law required to make the training fit reality has proved really challenging.

[1] Known as "Data 101" videos NB Records management and data quality "Data 101 videos" are completed and about to be released.

To compensate for this we are seeking opportunities to collaborate with other law enforcement partners who are in a similar position (e.g. NPCC, NCA, other agencies) and build that assessment in (and then its application) in partnership using DDAT professionals from within policing, supported by external experts in training in this space; truly ground breaking in what it will underpin for all of policing in the future.

5.7. **Commitment Two - Using data better** – Last year we focused on data capabilities that will make the biggest difference but where our understanding and/or maturity was low; quality and sharing. This has a multitude of benefits; better decisions, more accurate insights, greater transparency about what we are doing (and how well we are doing it) etc.

5.8. This has meant most of the work this year has commenced or improved what we collect about the data itself ("data about the data") and rewriting how we generate, collaborate and sign-off Data Sharing Agreements (DSAs) with our partners. We have also on-boarded the Open Data Institute to advise and shape our Open Data Strategy; the first force in the UK to take this approach. These improvements have also addressed real and legacy problems subject to many audit recommendations and scrutiny in the past.

- **Data Quality** – We are now able to assess the quality of the data held within our core operational systems (and compare that nationally based on what we upload to the Police National Database). This information is critical to good governance as it underpins decisions, by the business Information Asset Owners, about how we best derive value form the data we hold and how reliable it is; who can access it, how we use or share it, what we should collect/invest in and how useful it is (and thus whether we should stop paying to keep it). This means that 2022/23 can now be focused on our Year of Data Quality (YoDQ). The YoDQ[2] takes a strategic and tactical approach to embedding data quality principles to make our data work harder for us by *getting it right*, it is also a key dependency for the full "Go Live" of future data systems; Connect, Command & Control, BSS etc.

- **Data Sharing** – Building on previous work to improve internal use of DSAs work in 2021/22 focused on partners understanding of DSAs; especially what is appropriate to share. This has had mixed results (see **Appendix C**). In short, where Local Authorities and partners have engaged with the wider-London partnership on data sharing, we have seen success. Where they have not, we still see risk in how information will be governed well after we share it. The successes have been underpinned by; alignment to a pan-London network of information governance specialists from many agencies/Boroughs and part-funding a Data Sharing Administrator with this network to expedite DSAs (and fills a gap for London). Whilst London Office for Technology & Innovation (LOTI) have produced incredible tools and awareness on the need for consistency, no one body has oversight of

[2] The benefits of YoDQ, from a risk perspective, are far greater than saying that improved data quality leads to better operational decision making – we will be in a stronger position to be able to also discharge our obligations under MoPI, Subject Access Requests and Freedom of Information Requests therefore reducing compliance, financial and reputational risk and underpinning legitimacy and trust.

Information Governance across London partnerships. Progress is hindered as a result. Concurrently, we have worked with Safe Stats to include more sanitised police data available to our partners as well as improving our external dashboard on the issues that matter[3] (homicide, use of force, use of Taser, stop and search etc)

- **Data Ethics** – We remain committed to introducing a dedicated role/advisor for data ethics, but have struggled to recruit despite two campaigns (one of which was joint with Counter Terrorism Policing who encountered the same challenge). The grade and pay offer for such a role is less attractive in a buoyant market. Despite this, we have continued our work to align key artefacts[4] to incorporate ethical questions at the "idea" stage of data processing and endorse the Open Data Institute's data ethics canvas as a good tool to follow for this. We do, however, focus heavily on a similar set of questions already in our data and equalities work. Data ethics is an area where law enforcement are collaborating nationally (via NPCC) to align our sector approach; we are working with RUSI and the Centre for Data Ethics and Innovation (CDEI). The MPS has a seat at the National working group and we expect progress here in 2022/23.

5.9. **Commitment Three – Technology for Information Governance** – Since last Oversight Board technology capabilities have been introduced or procured in the space of information and data governance.

- **Evidential Data Archive**[5] - The most important tech investment is now ready for use and will be "switched on" once the project to automate our Review, Retention and Disposal (RRD) of operational data is complete and our data quality improves; this year, prior to the "Go Live" of Connect and C&C. This will be a **"game changer"** for MPS information governance and cannot be underestimated for its importance for lawful and ethical use of AI, analytics and data science going forwards.

- **Management of DPA compliance** - We have also procured a system to **digitally manage our Data Privacy Impact Assessments** (DPIAs) to go live Q1 2022/23. Currently DPIAs are tracked via email and spreadsheets. We will be able to performance manage, review and risk assess data processing automatically. In the interim, for 2021/22 we have increased capacity in our DPIA and data sharing teams to assess, manage and reduce the backlog, quality and timeliness of these key products. We have also improved the technology which shows **case management of FOI and SARs**. Since Feb 2022 we have been able to track timeliness beyond the Data Office and can see difference in "turnaround times" and "complexity" of requests within the wider operational units. It will form a key part of our performance report to Data Board in 2022/23.

- **Record of Processing Activity** (**ROPA**) - We have built an **interim solution** to meet ICO requirements to have a ROPA for the MPS. Whilst

[3] Based on the Met Direction, Policing and Crime Plan and trends/themes identified from FOI requests

[4] Data Privacy Impact Assessments, Equality Impact Assessments and the Commercial & Business Case lifecycle

[5] A solution to allow us to store compliant data and remove legacy systems

future investment will be required, it provides the basis upon which we can collect the data we need and enables us to build a future set of requirements in this space (again, this is an area where law enforcement is unique in its needs under DPA 2018 Part 2 and 3).

- **Facial Recognition** - We continue to lead the way in Police use of FR and our information governance processes here are rigorous. In particular in the data we collect, its retention and use and its deletion. Potential for bias is at the forefront of our mind and is considered during the DPIA and EIA process (and under continual review). During 2021/22 we undertook significant diligence testing against the algorithm for live facial recognition (LFR), drawing on the National Institute of Standards and Technology (NIST) tests and its significant expertise. The MPS is assured that it uses a highly accurate algorithm as a result. However, there is a need to build on this assurance by undertaking further assessment in realistic operational conditions. We will do this during 2022/23. The goal is to gain further assurance that the MPS uses a fair and accurate LFR capability to help identify individuals of interest through testing in non-ideal, but realistic operational conditions, including obscuration such as mask wearing and evaluating the 'human in the loop' decision-making process to identify the impact human factors have on performance. All outcomes will be shared across policing. The work would fill a gap and the benchmarking exercise planned is vital; there is currently no agreed or standard test available to law enforcement to assess any potential bias in non-live FR system algorithms. As the MPS has done with its use of FR more widely, it will seek to engage with stakeholders to develop appropriate policy, safeguards and controls – including with MOPAC and LPEP. This will ensure the MPS continues to use FR technology in a way that is lawful, ethical and effective.

5.10. **Commitment Four - Expanding analytics capabilities** – This year the MPS has introduced a **data analytics apprenticeship**; professionalising further what our analysts do with a recognised practical qualification. This is critical to good information governance as high-risk data processing (which is essentially the core of analytics) needs robust thought and application of law and ethics to maintain public trust. **Training of this nature has never been delivered in policing before and is critical to consistency and transparency**. 40 analysts from across the MPS[6] have undertaken the course in three cohorts. **25 have already graduated.**

5.11. To enable this apprenticeship to happen we concurrently invested in the right environment for them to safely, lawfully and ethically operate. This has been challenging, not just due to COVID, but because the wider capacity of the MPS that we need to stabilise the current environment and build a viable, long-term solution has been focused on other major Programmes of work[7]. Nevertheless, our Data Engineers built a development area to test analytics projects and they built specialist machines with coding and analytics tooling on them which are "bookable" as needed for this work. **These tools were not previously available**

[6] Intelligence, Met CC, Engagement, Counter Terrorism, Fleet and Data Office

[7] Connect, Command & Control in particular

anywhere in the MPS; an amazing achievement that has allowed us to progress against the odds and do so in a compliant way.

5.12. One specialist analytics service which became live in 2021 is **Risk Terrain Modelling**[8]. 20 licenses are live across the MPS and it has made an instant difference in the planning and tactics for violence and other critical operational areas.

5.13. **Commitment Five - Data Governance & Privacy Rights -** MPS Data Board is now an established structure providing oversight, strategic direction and risk mitigation at Executive level across data management, high risk data processing, analytics, cyber security and privacy rights. The Board receives performance reports underpinned by weekly dashboards and metrics for internal business use. Dashboards on FOI and SAR performance are also well established (since 2020) on our external website and continue to be well received by the public and the regulator. (See **Appendix D** for an overview of information governance)

5.14. **Regulatory Assessment** - During 2021/22 we volunteered to take part in an ICO Audit. The three areas reviewed were all fundamental to our progress in information governance; (i) **Governance & Accountability** (ii) **Information Risk Management** and (iii) **Records Management**.

5.15. Our strategic approach and investment to DDAT, but data in particular, since 2019 has served us well here as we received a favorable assessment. It should be noted that there were 16 of the 87 recommendations which we could not fully accept as they would require investment, albeit work has started on all those areas. See **Appendix E** for more detail on this and the wider ICO Audit.

5.16. **The one *outstanding area* which has no work underway is data assurance.** As yet, this is not work we have the capacity to improve without a full review and assessment of costs, but is a considerable risk we recognise. We will be investing in **Cyber Security** in 2022/23 but the assurance of our information security is not part of that at this stage.

5.17. It should be noted that, in information governance terms, there is no greater scrutiny than an ICO Audit. The MPS is proud of the progress and step-changes we have made here. The findings for the three areas are summarised below.

5.18. **Governance & Accountability** – In ICO Audit terms this relates to the extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance with Part 3 of the DPA18 and other national data protection legislation, are in place and in operation throughout the organisation. Much of this Oversight Board report relates to these areas and the rationale for a "reasonable" assessment is clear.

[8] A branch of geospatial analytics that diagnoses environmental conditions that lead to crime (and other problems). RTM analysis brings multiple sources of data together by connecting them to geographic places. It adds context to 'big data' and forecasts new risk patterns for locations

5.19. **Information Risk Management –** The ICO determined they have a reasonable level assurance that the MPS has applied a "privacy by design" approach and manages information risks throughout the organisation in a structured way. Again, much of the foundations for that have been covered elsewhere in this report. What is worth reviewing since the last Oversight Board is the progress made on Data Privacy Impact Assessments which was subject to considerable demand and backlogs in 2020/21, introduction of a ROPA and allocation of Information Asset Owners (IAOs).

5.20. **Records Management** - The ICO grading here was "limited". The MPS holds personal information for millions of individuals. In 2021, we completed work to quantify the scale of this holding with a view to "bulk deleting" any records we should no longer hold (with the added complexity that some systems are so old that deletion was not factored into the system itself). Our July 2021 pilot on this concluded that deletion by any method (manual or automated) would only be possible in around 14% of cases. This is because so many individuals (53%) went on to reoffend and, very often appeared on other data systems nationally[9]. The risk of deleting information that we should *retain* has meant that auto-bulk-deletion is not currently viable and would undermine the very reason we have rules for RRD in the first place (i.e. MoPI as a response to the murder of Holly Wells and Jessica Chapman). This complexity is acknowledged by the ICO and they will review progress over the next twelve months.

5.21. A Transformation Project was initiated in September 2021 to seek out cost effective solutions to this problem which is expected to deliver full compliance with MoPI (RRD rules) in 2026. To do this there are dependencies on improvements in data quality[10], our speed of review, archiving (now possible due to the Evidential Data Archive) and deletion. Note; All other forces are watching the MPS in this space. No other force has developed thinking on automated RRD nor quantified the risk

5.22. We have, however, implemented a "red line" point to stop the "data holdings" increasing unnecessarily or adding to the scale of the challenge. All records generated in 2021 have to be submitted to an assessment to check the data is entered correctly and is archived and cross-referenced in the correct systems. This activity is audited from the Data Office.

5.23. **Privacy Rights –** In 2020 we invested in resources to respond to an ICO Enforcement Notice about a backlog of SARs. We were successful, resulting in removal of the Notice. Since then we have maintained good management in this area. Public requests have now gone up a further 60%. We cannot recruit and retain qualified staff quick enough to match this demand (a problem faced across the sector). Redaction of multiple forms of media area also a challenge; especially the rise in Body Worn Video and other "video" technologies the MPS has introduced in the last year. Whilst we have Action Plans in place, increased resources and are seeking redaction technologies (for video and text) the dip in

[9] The remaining 33% which could potentially be deleted would require record by record manual review to check if what retention period was appropriate.

[10] we need to know which records are linked before we can conclude they should be retained or disposed of

performance here will take at least 6 months to start to turn around. For latest figures see **Appendix F** or our external website.

6. Challenges and Forward Look

6.1. **Recruiting, retaining and developing talent** - the ability to attract and retain talent in the DDAT space across the public sector is a considerable challenge, although longer established technology roles are better understood. This is particularly acute where data expertise is required (management, analytics, science, ethics, privacy rights). This is compounded in law enforcement as we are subject to extra aspects of data protection and other laws relating to the use of data (e.g. DPA Part 3 and Investigatory Powers Act). The expertise in these areas is in even more limited supply. The MPS is not competing with market rates and is fishing in a very small pool across DDAT specialisms. Concurrent to the pay challenges and the paucity of skills in the market, data governance is more complicated and complex in the public sector. Whilst appealing to core values and a sense of mission is a strong attraction, the problems to be solved are not always attractive to those with the skills we want (especially data analysts who would rather work on good quality data sets with top of the range tools and applications). For the MPS this is most acute in the area of data management where our major technology Programmes do not have access to expertise in data law, and its practical application in policing (which causes a draw on the resources we do have in this space). In order to maximise the brighter and stronger future in this area for the Met, and ensure the front-line get the digital tools and data they need this year, we will need to address this challenge.

6.2. **Our Enterprise Architecture and "the Grey Estate"**- A number of reviews of our digital and data strategies will see a greater alignment in the acquisition of tools and technology to enable greater interoperability and consistency across the MPS estate. At present, we have added to the range of applications and tools available, which has improved specific point solutions, but has also made information governance more complex. We will need to reconsider our approach and oversight of enterprise and data architecture during 2022/23, particularly as there are some large technology deliveries in train.

6.3. The effort, support and focus on significant technology programmes has impacted on delivery of other key technology needs that will cement better information governance. This is not a problem of budget, but of capacity and skills. There is a risk that failing to stabilise current systems and platforms will mean delivery of analytics and data science is stalled[11]. We will need 'privacy by default' considerations applied retrospectively to some of our investments too; video and text redaction are an example being worked through for delivery in Q1 of 2022/23. Prioritisation of technology and applications that we now know will be required to "land" looming transformation Programmes will be needed. RRD is going to be critical, for instance, as is the ability to maintain corporate reporting and data analysis and auditing, post-those systems "going live".

[11] MetStats Stabilisation, IIP,

6.4. The risk presented by the instability of our **data analytics platform[12] and search function[13]** and future procurement of solutions for reporting & analytics platform and enterprise search remains; capacity challenges presented due to significant technology changes for Transformation Programmes, but will be a priority for 2022/23 if we are to accelerate our ambitions for DDAT.

6.5. Added to the increasing complexity of "new" technology procurements is the "legacy" of the **grey estate**; systems, applications, platforms, and equipment (servers, networks, end-user devices) unsupported by DP. There are 305 such items in the MPS. AC Rolfe is leading on reducing and removing the risk presented by these items. Critical to that will be an assessment of a) their compliance with Data Legislation and b) our obligations to review the data within them against MOPI (as above, the decision to RRD each record is complex and just because a system is not compliant the data may need to be retained). Past and future decisions on technology procurement have a direct impact on data quality, data governance and data compliance. We will work hard in 2022/23 to support the proposed enterprise-wide view of change to remove the risk presented by future investments and strengthen digital and data governance processes to avoid wasting time, effort and finances on unpicking single-point solutions that risk undermining the wider effort of the organisation.

6.6. **Digital & Data** – In order to maximise and accelerate our activity to bring better data for decision-making to front-line decision-makers, operations and organisational investments we will need to better align Digital and Data priorities and that to incorporate DDAT as a whole (Data and Analytics sits with the Data Office/Board, Digital and Technology sits across Transformation Directorate and DP). We will start this by aligning our governance structures and removing duplication within it and resetting joint strategies to aid prioritisation. Management Board will be considering a joint Digital and Data plan in May. We are aiming to move to a joint Digital and Data Board in September.

6.7. **Data Literacy and Professionalising DDAT**– There are three concurrent achievements needed here to progress our ambition through good information governance (i) Establishing Information Asset Owners, (ii) building the skills and career framework for DDAT Professionals and (iii) maturing the awareness of data in our frontline and senior leaders.

- **Information Asset Owners** - In the last year we have built an IAOs handbook, educated all the IAOs (MPS Commanders) on their role, generated a contract between Data Office and the IAOs so roles and support accountabilities are clear and generated Data Health reports to drive decision-making. Our intention had been to launch an IAO Portfolio meeting as a sub-group to Data Board; that has stalled as nearly all of the people occupying those roles have changed in February and March. This will now be launched Q1 2022/23.

- **Work on a DDAT professional framework** – that mirrors the cross-Government framework – will need to build on work commenced in 2021. We are undertaking benchmarking in this area and it will be vital to underpin consistency of skills and

[12] Colloquially known as "MetStats"
[13] Colloquially known as "IIP"

help address the “talent” challenge outlined above. We will expand the number of licenses in use for Risk Terrain Modelling and the Data Science Apprenticeships across the MPS and we will welcome our Head of Data Science (advertising now) to provide professional direction.

- **Wider literacy** - across wider-MPS roles (i.e. front-line and staff and senior decision-makers) we will continue to simplify access for them to get advice, support, tools and data to do their jobs. We will extend our suite of “101” videos that are used at the point of action[14] and refresh our Information & You training.

6.8. **Open Data Mind-set –** We have commenced work on an Open Data Strategy. This will bring significant benefits to; rebuilding trust, our openness and transparency, provision of data and insight that improves our engagement with the public and reducing demand for information (e.g. via FOI or partners requiring data sharing agreements). To achieve this, we will need a shift in our leaders mind-set to support the broadening of the information we share via our website, through the use of dashboards and in the anonymised data we may ingest into collaborative platforms (such as safe stats). Policing is, for obvious reasons, a need-to-know organisation. This will not change for information relating to investigations, intelligence etc. Having an Open Data Strategy is about the data we present to maintain and improve our legitimacy with the public. In addition to the benefits of being an appropriately open-data organisation we should mitigate the perceived reduction in “openness” that may come from the removal of direct access to our operational systems as a key activity leading up to the launch of Connect. We cannot sustain the majority of the external party access, given regulatory direction, learning from previous breaches by 3rd parties and the necessary information governance of an “all in one” operational system. We will be withdrawing access where necessary during 2022 as a result and that may prove uncomfortable.

6.9. **Legislative and Regulatory Reform –** The MPS and Counter Terrorism Policing have been at the heart of influencing data protection reform and the review of Investigatory Powers Act. We are also leaning into the Online Safety Bill and Police, Crime and Sentencing Bill. Along with our NPCC colleagues we know that the combination of reform in this space will dramatically change what we will/won’t be able to do with data going forwards. We are confident that many of the barriers we have sought to remove are being taken forward with DCMS by the Home Office. If adopted in the final Bill it will mean improvements in how our front line can use data. The challenge is the timing of the need to respond to those changes through our information governance (i.e. our policies, processes and operational activity). The DPA reform, in particular, will be before the House in the summer; our response to this will overlap with the delivery of large Programmes of Technology delivery.

[14] “How to…fill in a DPIA”, “Using Dashboards”

Appendix A – Data Maturity Profile to ensure good information governance in the MPS

Where were we – 2019	Where are we now - 2021	What we do next - 2023
Most complained about organisation in the UK for Privacy Rights 3 ICO Enforcement Notices • Gangs Violence Matrix • Subject Access Requests (DPA 1998 & DPA 2018). • 2000+ backlog for and 30% compliance with new requests SIRO in place and Information Assurance & Security Meeting manages risk Prevailing culture about data is about performance. Data is a "hindsight" tool to inform Inquiries. Limited completion of our mandatory training on Data Law. A Transformation Programme is underway to improve data capabilities. This includes investment in a Data Office and Data & Analytics Strategy	Data a core pillar of our Business Plan and Strategy (Met Direction) Privacy Rights performance (FOIA & DPA) is published externally No Enforcement Notices remain. Strong relationships with ICO (and IPCO, SCC and Biometrics Commissioner) Data Board hosting the SIRO, oversees the Data & Analytics Strategies & risk management Director of Data in post managing first Data Office in Policing. A model other forces and agencies are keen to follow Prevailing culture about data is that it is recognised as important, staff are keen to learn. Nearly 90% of MPS Personnel have completed mandatory training. Maturing capabilities – • Information Asset Register in place • Information Asset Ownership is building • Analytics apprenticeships • Self-service reporting tools for frontline & operational staff (MetInsights, DES and dashboards) • Data Ethics lead recruited • Able to track core MPS data performance (compliance, quality and breaches) • Data literacy curriculum build; embedding into all levels of training/promotion • Managing the risk of our legacy versus our ambition – Project to RRD critical legacy assets[15] • Intranet campaigns & bite size videos to raise frontline awareness • Process improvement, and procurement of digital solution, to manage DPIAs and Data Sharing Agreements (the latter in partnership with London Authorities) Strong national voice & leadership on data/analytics alongside biometrics and facial recognition, including data protection reform.	Capabilities that will be in place/matured *Training & Awareness* • Data is part of the curriculum at all levels of the organisation *People/Skills* • Data Science capability in place • Analytics and some AI a part of operating practice • Career pathways for data professionals across the MPS and wider Law enforcement (interchange and growth of talent) *Technology* • Integrated digital data solution in place (Connect, Command and Control) • Stabilised data environment and improved reporting & analytics tools • Building Enterprise search *Transparency & Privacy Rights* • Open Data Strategy in place – more data in the public and partner domains (self-service and context) Prevailing culture about data is that it is a valuable organisational asset; using data to drive strategic and tactical decision making to police London (crime prevention, detection and outcomes, proactive targeting, productivity, investment choices, impact/benefit analysis)

[15] Review, Retain and Dispose (i.e. compliance with MOPI) in our core operational systems

Appendix B – Data Accessibility tools launched in the last 12 months

Launch of a **Data Portal**[16] where frontline can access all data tools in one place. Critically this includes **web-based Geographic Information that is automatically geocoded from our operational systems** – you can plot crimes or calls and use them to investigate or analyse a problem (such as plotting an area for a knife-sweep, or looking at 'travelling time', and locations of interest, from the last known sighting of a MISPER). Not only is this opening up thousands of records to investigators, it is *saving hours of time* not having to geocode for individual circumstances every time.

Broadening the access to **self-service report building** – through Met Insights and MetStats2 – both tools which enable officers and analysts to build queries and reports across operational data sets. We have also strengthened these tools by adding more data sets too – improving the readiness of the data available, as well as its accessibility.

The review and consolidation of all **operational dashboards** into one place. This included a data compliance review of all dashboards to ensure personal data was not accessible unnecessarily. Since these improvements, **dashboard usage has increased 25%**[17]. Feedback from frontline users, and senior decision-makers, is very positive. The reports most often used (daily) are Offender Management, BCU Performance and Police Officer workload[18]. From an information governance perspective, this means we have a consistent source of data for decision-making and review.

Appendix C - Data Sharing Agreements with London Partners[19]

Collectively the MPS and their partners work with operational roles to draft relevant sharing arrangements onto a standard digital template (NB replacing the 32+ templates we used to have in previous scenarios) that is accessible on a standard tech platform. These are *electronically* signed on behalf of each Data Controller by a senior rep in each agency. Critically, they can be adapted as operational sharing needs change and can be reviewed periodically from an assurance perspective.

Gangs Violence Matrix	30/32
Multi-Agency Safeguarding	20/32
Integrated Offender Management	3/32
Multi-Agency Risk Assessment Conferences	Just commencing digital sign-off
Multi-Agency Public Protection Arrangements	Under final review before sign-off
Youth Offending Services	DSA under formulation
Adult Safeguarding	DSA under formulation

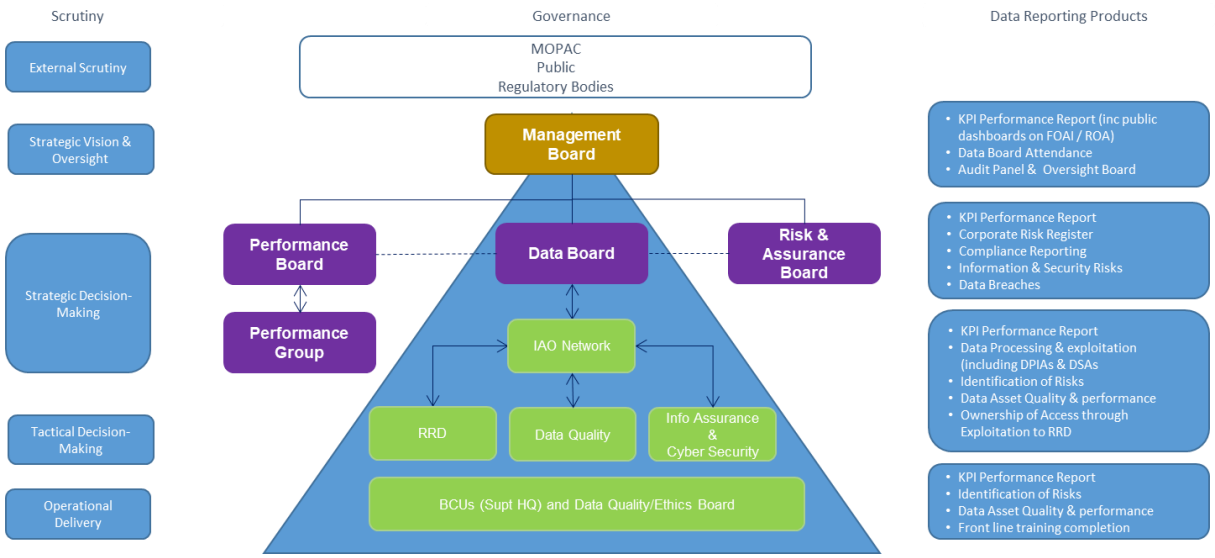
[16] March 2021

[17] Feb 2021 compared to Feb 2022

[18] March 2022 – 7000+ hits

[19] As of March 2022.

Appendix D - How Information & Security Risk Management is overseen



Appendix E – Overview of the ICO Audit into MPS

The ICO Audit team conducted work over a 12 week period and received over 500 documents to cover 182 requirements (99% of requested documents), interviews of circa 40 people including Management Board members and an MPS-wide ICO survey with approx. 2,800 completions.

We received a favorable assessment[20] especially compared to the 14 other forces and related agencies already audited in this sector. Of particular note was the assessment of "reasonable" on our Governance and Accountability (on a scale of; very limited, limited, **reasonable**, high). We were issued 87 recommendations, only 2 were urgent priority (both relating to records management and the need to align LDSS and Data Office processes and resources)

We are managing our response to the recommendations through a Working Group and have already had our three month progress check with the lead auditor. Progress is graded as good and on track.

There were 16 recommendation which we only partially accepted to complete as they would require further investment of resources and money to fulfil. Broadly these relate to system access improvements (especially 3rd parties), data mapping, collecting robust "data about data", wide-spread data literacy and fulfilment of RRD – we have started work on all of these areas (as noted within this paper). Future investment linked to these areas will be considered by the MPS in due course.

[20] Governance & Accountability – Reasonable, Information risk Management – Reasonable, and Records Management - Limited

Appendix F – Privacy Rights Performance

- In 2021, we received 12,237 ROA requests (up from 10,207 in 2020 and 7,700 in 2019). On average across the year we responded to these in a timely manner in 69% of cases[21]. In 2020 our yearly average was 71% (in 2019 it was 40%).
- There are currently 1,152[22] open ROA requests on our system. 921 are overdue (80% of open requests are overdue). The oldest case is from 09 April 2021.
- In 2021, we received 4,941 FOI requests (4,233 in 2020 and 4,388 in 2019). On average across the year we responded to these in a timely manner in 70% of cases[23]. In 2020 our yearly average was 72% (in 2019 it was 60%).
- There are currently 456 open FOI requests on our system. 175 ae overdue (38% of open requests are overdue).

[21] 8,181 of 11,848 requests NB some ROAs will be rejected and not dealt with

[22] Correct as of 07 March 2022

[23] 3,298 of 4,719 requests NB some FOIA will be rejected and not dealt with