Freedom of Information Act Publication Scheme	
Government Security Classification	Official
Publication Scheme Y/N	No
Title	A purpose specific Data Sharing Agreement (DSA) between DPS Reviews Team and MOPAC CRT
Version	Version 1.0
Summary	An agreement to formalise data sharing arrangements between DPS Reviews Team and MOPAC CRT for the purpose of MOPAC CRT carrying out regulatory obligations of conducting Review assessments (appeals) into public complaints (S.29 Police Complaints and Misconduct Regulations 2019).
(B)OCU or Unit, Directorate	Directorate of Professional Standards, Reviews Team
Author	Inspector [redacted]
Review Date	17/11/2021
Date Issued	17/11/2020
CycFreedom Reference	01/DPA/20/000780 (DPIA 01/DPA/20/000664)

Purpose Specific

Data Sharing Agreement (DSA) Between The MPS and MOPAC Police Complaint Review Team

This document is a re-write of the previous DSA between DPS Reviews and MOPAC CRT following a COG decision to change access levels to relevant cases.

Template Version 2.0

Table of Contents

Section 1. Purpose of the Data Sharing Agreement

The purpose of this DSA is to agree formally how Personal and or Special Category Data shared between the MPS and Partner Organisation(s) will be processed and used.

By signing this agreement, the named agencies agree to accept the conditions set in this document, according to their statutory and professional responsibilities. They also agree to adhere to the procedures described herein, which are to:

- Define the specific purpose(s) for which the Signatory Organisation(s) have agreed to share data;
- Outline the Personal and or Special Category Data to be shared;
- Set out the legal gateway through which the data will be shared;
- Stipulate the role(s) and procedures that will support the processing of data between the Signatory Organisation(s);
- Describe how the rights of the data subject(s) will be protected as stipulated under the following Data Protection laws: General Data Protection Regulations (GDPR), and the Data Protection Act (2018) (together Data Protection Legislation);
- Describe the security procedures in place to ensure compliance with the Data Protection Act (2018) and Partner Organisation(s)-specific requirements;
- Describe how the Signatory Organisation(s) will monitor and review this arrangement.

The parties also agree that they will comply with their respective obligations under applicable Data Protection Legislation.

The signatories to this agreement will represent the following agencies:

- MPS, **Directorate of Professional Standards** (DPS Reviews Team) &
- **MOPAC, (MOPAC CRT)**

Section 2. Background to initiative and what data you plan to share

2.1 Purpose and Scope for sharing data

Q1. Provide the background to this initiative and explain what this project is about:

The background to this information sharing agreement is the reform legislation and regulations that cover the handling and review of what are currently referred to as '*Reviews*' (since 1.2.2020) and previously known as '*Appeals*'.

The specific legislation is the Police and Crime Act 2017 and the Police Complaints and Misconduct Regulations 2020, (PCMR). These are legislative reforms which move the responsibility for being a Relevant Appeal Body from forces (Metropolitan Police Service) to Relevant Review Body by the Offices of Police Crime Commissioners (MOPAC in London). To support this legislation there are new and updated Police Regulations which support this legislation as well as statutory guidance from both the Home Office and the Independent Office for Police Conduct, (IOPC)

All public complaints are initially dealt with by Force unless they are deemed to fall into the referral category for the IOPC. Each public complaint is then handled according to its severity and complexity and an outcome is provided. With the outcome, details of the Relevant Review Body and the right to review are given. This will either be the IOPC or MOPAC. If the complainant is still not satisfied with the information received they can exercise their right of review. In order to accomplish this the MPS will need to provide details of and background papers to public complaints which, contain both Personal Data and Special Category Data. The background material to a complaint will often include Body Worn Video, which also contains Special category data. It therefore follows that records which are created and edited by the MPS will need to be shared with MOPAC in order that they can effectively discharge their role as a review body in conducting reviews.

MOPAC shall not share data provided to them by the MPS in support of their role as the review body with any other party unless MOPAC has a lawful basis for doing so.

Q2. Explain briefly what this project aims to achieve:

The aim of this DSA is to agree and sign up to data sharing and to describe how that will happen between the MPS Reviews Team (who currently conduct force appeals as well as servicing IOPC appeals data requests) and MOPAC CRT, who are required to replicate at least some of the responsibilities of IOPC. (Conducting Reviews and making Recommendations – Reg.28 PCMR 2020). In short, if any of the RRB receive a review request which does not fit their remit, the RRB must forward it to the relevant authority.

It is to ensure that the MPS shares information in the most appropriate, proportionate manner by the most appropriate means in order that MOPAC CRT can discharge their legal obligations to conduct reviews of public complaints.

It is proposed that MOPAC CRT are given access to the MPS DPS Centurion complaints and conduct system in order to facilitate the sharing of information/data so that they can conduct reviews. MOPAC CRT will only have the ability to search and review all public complaint cases. (cases designated with the prefix PC on the system and some with IX prefix for cases created during the last major system upgrade). MOPAC CRT will not have the ability to delete any data. MOPAC will not have the ability to print hard copies. They will only have the ability to read and add.

The proposed method that this takes is by MOPAC CRT using the MPS licence access to Centurion in agreement with F.I.S (Force Information Systems) the company that provides Centurion, and there being in place the appropriate search access for public complaints, so that MOPAC can access any cases where they are the Relevant Review Body or have a requirement to review the material for a Review that they are the RRB for (linked cases). In short, MOPAC CRT can use MPS licences and will not have to apply to the makers of the Centurion system, for their own licenses.

In order to ensure the complainant understands what the MPS will do with the personal data, there is a data sharing disclaimer on all DPS correspondence to new complainants which informs them that we will use their data in order to provide them with a complaint outcome and that we will share it with other public bodies as required in order to facilitate their rights to review. Those public bodies are MOPAC and where necessary the IOPC. .

Q3. Confirm what type of data you will be using i.e. Personal and or Special Category[1]:

The type of data that will be required to be shared will be both Personal and Special Category data. MOPAC will be required to review any and all material that was used in the consideration of a public complaint.

Q4. Provide a clear list of the data that the Partner Organisation(s) is requesting from the MPS and label which ones are Personal and or Special Category Data:
e.g. information on crimes, terrorism, anti-social behaviour and public order

MOPAC may request relevant extracts of the following data, if it can not be located on Centurion. Key documents are normally held on Centurion, but back ground material including email trails etc is held on locally on the Shared Drive.
This position will change in future when PSUs have their own access to Centurion. All relevant materials will be saved to Centurion at source.

MPS will provide MOPAC CRT with access to:

- Public Complaint Records – Personal data & Special Category data
- Body Worn Video – Personal data & Special Category data
- Other camera footage both police owned and public – Special Category data
- Extracts of Police Crime Reports – Personal data & Special Category data
- Extracts of Police Intelligence reports – Personal data &Special Category data
- Extracts of Police Safeguarding reports – Personal data & Special Category data
- Policy, SOPs and Local Instructions.
- Witness evidence – Personal data & Special Category data

Information (material) which becomes part of a Public Complaint case & review can be formed with

[1] **Personal Data**: Data relating to a living identified or identifiable individual, including: a person's name, address, dob, email address, telephone number, id number, bank and credit card details, location data, online identifier or one or more factors specific to someone's physical, physiological, genetic, economic, cultural or social identity.

Special Category Data: Data that reveals a person's racial, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics, health, sex life / orientation, criminal convictions and offences, related security measures or appropriate safeguards. This includes photographs and CCTV images.

data held in any MPS system. Therefore, in relation to the reviewing of Public Complaint cases, MOPAC CRT will have access to various types of personal data, as described by GDPR Article 4(1) and the footnote below.

Q5. Provide a clear list of the data that the MPS is requesting from the Partner Organisation(s) and label which ones are Personal and or Special Category Data:

- MPS will not be requesting data from MOPAC
- MOPAC will use MPS data in order to discharge their legal function as a review body.

Q6. Explain the benefits of this sharing agreement for: MPS & MOPAC

a) The MPS:

- The MPS are legally obliged under the new legislation (Police and Crime Act 2017, Police Complaint and Misconduct Regulations 2020, IOPC statutory guidance) to provide any information that the review body deems necessary in order for them to discharge their duty. It will allow the MPS to meet this legal requirement whilst ensuring the security of the data and also adherence to DPA principles.

b) The Partner Organisation(s):

- MOPAC are legally obliged under the new legislation to take on the role of review body – to conduct Reviews of public complaint outcomes. The details of these complaints will have been created and updated on the MPS Centurion system. They would have been dealt with as a public complaint and an outcome reached. If MOPAC have to conduct a Review then it will be as a consequence of a member of the public exercising their right of Review (appeal) over the handling or outcome of that complaint.

c) The Public:

- Effective and efficient review of public complaints
- Ease of dealing with such complaint reviews
- Increase in timeliness to conduct reviews due to streamlined working

2.2 MPS Data to be shared

Q7. List the MPS systems the data will be taken from and the relevant fields in these systems you intend to use:
i.e. ***CRIS*** *– name, address, details of investigation found on DETs page,* ***PNC*** *- disposable history.*

The MPS will permit MOPAC CRT to access the Centurion system, to review all cases marked with the Prefix PC or IX, which are relevant to MOPAC for discharging its function as a Relevant Review Body (RRB).

Caveat – it will not be system access to the below but will be relevant extracts of -

- CRIS system – Name, Address, date of birth, gender, ethnicity, details of investigation, Victim, Informant, Witness, Suspect, Accused.
- CrimInt database - (subject to harm test) relevant extract details
- Merlin database - (subject to harm test) relevant extract from details
- CAD system – All fields
- IIP database – all fields
- Any other police indices – Relevant fields for the purpose of identifying witnesses or contacting complainants.

Q8. State the reason(s) why it is necessary to share this data with the Partner Organisation(s) and what the impact would be if it was not shared:

It is necessary to share this information as there is a legal duty placed upon the MPS under Regulation 29(7) Police Complaints and Misconduct Regulations 2020 to facilitate the provision of any relevant information or data which will enable MOPAC CRT to discharge their duty as a relevant review body and the assessment of review applications.

Q9. Please confirm the following:

MOPAC will not disclose MPS data shared under the terms of this agreement with a third party unless MOPAC has a lawful basis for doing so.

If the answer is no, please explain why:

n/a

Q10. If a third party will access MPS data, then the ISSU will need to know about the process used to make it available to them and how they will process it.

If this question applies, please explain how this data will be shared with a third party and what that party will do with it:

n/a

Q11. Will the MPS data shared under the terms of this agreement remain within the European Economic Area (EEA)?

Yes – MOPAC CRT will have access to DPS's system, Centurion. Servers are UK based.

If the answer is no, explain how will you safeguard any international transfers:

n/a

2.3. Consent

Explicit consent must be sought from data subjects where it has been identified as necessary for the processing of personal data, as stipulated in the relevant Data Protection, GDPR, , and policies of the Partners of this agreement.

Where consent is required, it is the responsibility of the Partner Organisation(s) to seek it from the data subjects. Individuals should be made aware of how their personal data will be processed, why and which agencies it will be shared with. They should also be informed that they can withdraw their consent at any time.

In circumstances where consent has been refused or withdrawn by the data subject, that data must not be used, unless withholding it would risk causing harm or distress to another party. Nevertheless, there may be occasions where personal data may be legally shared with other agencies without consent.

Q12. Please confirm the following:

MOPAC CRT will seek the explicit[2] consent of its data subjects:

No

If the answer if no, please explain why:

The Complainant has exercised his/her right under the PCMR 2020 to request MOPAC to review the Outcome of the MPS handling of their complaint. In addition there is a data disclaimer on the correspondence for first contact with DPS as detailed in bold below:

[2] Under the Data Protection Act (2018) consent must be obtained by a participant opting in. It cannot be implied or assumed and it must be for a specific purpose.

The information you have provided in this form will be used by public bodies involved in the police complaints system including other police forces and the Relevant Review Bodies, MOPAC & IOPC who will use this information in order to review the handling of complaints by the Metropolitan Police Service under the Police and Crime Act 2017 and the Police Complaints and Misconduct Regulations 2020.

Q13. Please confirm the following:

MOPAC data subjects will be made aware of how their personal data will be processed.

Yes

If the answer is yes, please explain how the Partner Organisation(s) made them aware and if the answer is no, explain why:

This is covered in MOPACs own privacy notice which is available online and via the link below;

https://www.london.gov.uk/what-we-do/mayors-office-policing-and-crime-mopac/about-mayors-office-policing-and-crime-mopac/mopac-complaints

Any requests pertaining to matters prior to 01-02-2020 do not fall within the authority of MOPAC and will be forwarded to DPS Appeals as per relevant legislation. (All review/appeal bodies have a duty to forward misdirected appeals/requests for review to the relevant authority)

2.4. Common Law Duty of Confidentiality

If information is provided in confidence to one of the signatories of this agreement then they have a Duty of Confidentiality towards the data subject that it concerns and can only share this information if they have a compelling reason (i.e. in the public interest) to do so.

Q14. Confirm the following:

The Partner Organisation(s) has a duty of confidence towards its data subject(s):

Yes

If the answer is yes, explain what legal reason would they use to justify disclosing this data to a third party:

The duty of confidence can be overridden by MOPAC, if the data subject explicitly consents. Otherwise it is for MOPAC to establish their own legal basis for overriding any duty of confidence. MOPAC is responsible for justifying any such disclosure to a third party.

MOPAC CRT have direct access to the MPS system Centurion for public complaints and no longer have to request information from the MPS (DPS Complaints). Before the direct access was given to MOPAC CRT, each occasion where MOPAC CRT requested information about a specific case, directly disclosed to the MPS that the Complainant has exercised his/her rights under PCMR 2020 and PCA 2017.

In future, MOPAC will still inform the MPS when a complainant exercises their right of review as this is a

requirement of PCMR 2020.

3. Privacy Management & Security Framework

3.1 Data Sharing Process

Requests for MPS data

Q15. Please explain the following:

a) How will the Partner Organisation(s) make requests for MPS data?

MOPAC CRT will make any further requests for MPS data by email.
In relation to Centurion records, MOPAC CRT will be given direct access to all Centurion cases relating to public complaints. This will enable them to determine Relevant Review Body authority, consider duplicate complaints and vexatious complaints as well as the assessment and review of complaints for which they have received requests for Review.

MOPAC will make requests for data in writing to the relevant department, for any additional data which is not attached to Centurion records. MPS will give MOPAC access to all information it requires in order to discharge its function as an RRB.

b) Who [job title] within the Partner Organisation(s) is responsible for making these requests?

The MOPAC CRT will make the requests for data on behalf of the Deputy Mayor for Policing and Crime who is the de facto PCC for London.

c) State the means by which these requests will be made:
i.e. via secure (state the type) email, post, phone:

Requests for data must be made via email in order to maintain a clear audit of requests and what is shared.

Q16. How will the MPS gather the data requested?

The MPS (DPS Complaints) will send an email to the local PSUs on BCUs, to gather any data for the purpose of this DSA.

Who will be responsible for doing this?

MOPAC CRT will be responsible for completing these data requests.

Q17a. Who is the MPS's primary point of contact [job title] within the Partner Organisation(s)?

- [redacted] - Staff – Seconded to MOPAC – MOPAC head of Professional Standards and Workforce.

b) Who are the recipient(s) of MPS data within the Partner Organisation(s)?

- MOPAC CRT

c) If there is a secondary point of contact, state who it is?

- [redacted] MOPAC CRT Manager

Q18. Is there a requirement for the Partner Organisation(s) to have access to MPS ICT systems?[3]

Yes

If so, state which systems, who [job title] specifically will have access to them and why they require it:

MOPAC CRT will be given direct access to Centurion. This will enable them to conduct their own system searches for public complaints. Within MOPAC, the access would be limited to only members of their complaints review team which will be a maximum of TEN people. **MOPAC CRT have been issued with MPS Laptops which enables them to access Centurion.**

"All usage of MPS systems will be audited in line with MPS and national standards. MPS managers will ensure a suitable level of supervision is provided". This is an operational need as direct access can only be granted by the use of MPS devices.

MOPAC have a further statutory role defined by the Police and Crime Act 2017 This DSA does not cover that responsibility which is governance and oversight and the handling of complaints against the Commissioner.

[3] This should only happen when it is operationally imperative to share data and there is no other means available. If access will be granted to personnel from a Partner Organisation, please include the following text: "All usage of MPS systems will be audited in line with MPS and national standards. MPS managers will ensure a suitable level of supervision is provided".

Requests for MOPAC Data

If the MPS will also receive data from the Partner Organisation(s) then complete the following section.

Q19. Please explain the following:

a) How will the MPS request data from the Partner Organisation(s)?

N/A The MPS will not request data from MOPAC CRT for the purposes of this DSA.

However, MOPAC are required to provide us with a copy of the final review assessment, as we are an interested party and therefore are entitled to this, especially if there are recommendations within.

b) Who [job title] is responsible for making these requests?

N/A

c) State the means by which these requests will be made:
i.e. via secure (state the type) email, post or phone.

N/A

Q20a. How will the Partner Organisation(s) gather the data requested?

N/A as the MPS will not request data from MOPAC CRT for the purpose of this DSA.

b) Who will be responsible for doing this?

N/A

c) Which systems will be interrogate?

N/A.

Q21a. Who is the Partner Organisation(s)'s primary point of contact within the MPS?

- [redacted] MPS Staff on secondment to MOPAC.

b) Who are the recipients of the Partner Organisation(s)'s data within the MPS?

- DPS Reviews Team.

c) If there is a secondary point of contact, state who it is?

- [redacted] **MOPAC CRT Manager**

If MOPAC CRT requests further information which was not part of the MPS's initial review of the Public Complaint, The **MPS SPOC** **MPS Reviews Team** will create a record of any personal data disclosed to **MOPAC CRT** on CENTURION (within the relevant case), at the time the data is supplied (or as soon as possible thereafter). This should include what was shared or not, and the reason for that decision. The system is subject to regular auditing.

3.2 Confidentiality and Vetting

Where OFFICIAL SENSITIVE data is being shared, vetting is not mandatory but access must be, limited to those that "need-to-know" (in this case MOPAC CRT) (unless there are national security implications, in which case a Counter Terrorist Check (CTC) is required). **MOPAC** must confirm that they have provisions in place designed to ensure that unauthorised dissemination or copying by their staff (MOPAC CRT) does not occur.

Q22. Have employees in the Partner Organisation(s), who receive MPS data, undergone any vetting?

Yes

If so, please state to what level:

MOPAC report that the all members from the MOPAC CRT who require access to the MPS system Centurion are Counter Terrorist Check (CTC) vetted. This will be a maximum of TEN staff members. This differs from MPS staff because MPS staff have access to more than just public complaints which are marked as MoPI Group 3 & 2.

MoPI Group 3 = 6 years retention – if longer review 5yrs
MoPI Group 2 = 10 years retention – reviewed after every 10yr clear period (ie has not come to notice)
MoPI Group 1 = 100 years retention – reviewed every 10yrs

And remember MOPAC staff are not employees of a Competent Authority – MOPAC have no law enforcement functions = Part 3. DPA 2018, they only have statutory function = to GDPR.

Q23. Does the Partner Organisation(s), require their employees to sign a confidentiality agreement, or an equivalent level of assurance of confidentiality?

No

If the answer is no, please explain why such measures are not required:

All members of the MOPAC CRT will be subject to vetting to the CTC level. They also sign system use agreements which reminds them of their obligations and liabilities. There is a confidentiality requirement within their contract of employment.

3.3 Data Transfer

Hard Copy

No hard copies are produced or transferred.

Electronically

- Data marked with a Government Security Classification up to the level of OFFICIAL SENSITIVE will be transferred using either Centurion workflow or via TLS1.2.
  Both the MPS and MOPAC have Government security rated secure email systems.

- If information is to be shared over the telephone, speech will be guarded and conversations kept short.

- The use of fax for transferring data marked OFFICIAL SENSITIVE will be avoided, as it is not secure. If this is the only option, the guidance specified in the *METSEC Code* will be followed. However, data marked higher than this will not be transferred in this way. This method is unlikely due to the two teams being co-located and the lack of fax facilities within the unit.

3.4 Data Storage

Partner Agency's Building & Perimeter Security

MPS data must be kept within a secure location with a managed and auditable access control system that the general public will have no access to.

Hard Copy

Q.24. Explain how the Partner Organisation(s) will store hard copies of OFFICIAL SENSITIVE MPS data: *N/A as the MPS do not send Hard Copies to MOPAC. All the information which MOPAC CRT will need access to, is held in the MPS Centurion system which MOPAC CRT have direct access to.*

Electronically on a Partner's system

Q25. Explain what system access controls the Partner Organisation(s) has in place to keep MPS information safe: MPS information is contained in Centurion only. We invite MOPAC CRT in, we do not send data out.
Q26. **MOPAC** confirm that the MPS can audit the data they sent to them at any time. N/A

If the answer is no please state why:

N/A - as the MPS do not send data to MOPAC CRT. All and any further information which is required by MOPAC CRT will be located and entered into Centurion for their use. MOPAC CRT has direct access to Public Complaints data which is held in Centurion. MPS Centurion is fully auditable, so there will be an audit trail of MOPAC CRTs access and use of the MPS Centurion system.

Q27. MOPAC is part of the UK Government Cyber Essentials scheme.

N/K – It is a founder of the London Digital Security Centre, is a key strategic partner to numerous public bodies and organisations and holds many statutory duties so will likely be a member.

If the answer is yes, please provide the date when they joined.

MOPAC came into being on 16/01/2012, arrangements would have been required from this time.

3.5 Business Continuity

If the data shared within this agreement will be backed up, either electronically or with the movement of physical files, then the responsible party must ensure that the appropriate storage and protection measures are in place to comply with their obligations under Data Protection Legislation.

Electronically

If data is backed up electronically via a hard drive, or any mobile device, then the appropriate level of encryption and or password requirements to comply with the party's obligations under Data Protection Legislation must be in place. This device should also be stored in a physical location with the same level of security as the data being held.

Hard Copy

If data shared under this agreement must be moved from its usual secure location, which is in accordance with the level of security required by this agreement, then any move temporary or permanent must provide the same level of security in storage as originally agreed and stated in this document.

Whilst the Partner Organisation(s) may have their own security standards & protocols, where MPS data is concerned the relevant security standards set out by the GSC for transmitting, storing and disposing data must be adhered to at all times.

3.6 Data Destruction / Disposal

Hard Copy

N/A as no hard copies are sent to MOPAC, and disposal by cross shredder is not necessary.

Electronic Information from Partner's System

N/A as data held within MPS Centurion.

3.7 Reporting Security Incidents and Breaches of the Agreement

Partner Organisation(s) Responsibility

Security breaches, including misuse of MPS data, must be reported to the MPS SPOC **[The DPS Complaints SPOC]** without undue delay of occurring/or no later than 24 hours after the MOPAC CRT becomes aware of it. This is to allow the MPS to risk assess the security incident or breach of this Agreement.

The nominated MPS SPOC **[The DPS Complaints SPOC]** will also **immediately** inform the Information Assurance Unit (IAU) of any security incidents or breaches of this agreement, including unauthorised disclosure or loss of data, by emailing 'IAU Mailbox - Security Incidents'.

However it is still the responsibility of [MOPAC] to comply with the obligations laid out under Section 67 and 68 of the DPA 2018.

It is also confirmed that security breaches including misuse or unauthorised disclosure, are covered by **[MOPACs]** internal disciplinary procedures. If misuse is found, there should be a mechanism to facilitate an investigation, which includes initiating criminal proceedings where necessary.

It is also confirmed that security breaches including misuse or unauthorised disclosure, are covered by MOPAC internal disciplinary procedures. If misuse is found, there should be a mechanism to facilitate an investigation, which includes initiating criminal proceedings where necessary.

MPS Responsibility

Q28. Detail the process MOPAC would like the MPS to comply with should a security breach occur on our part:

1. Immediately and no later than 48 hours, the unit discovering the breach would inform the senior member of the MOPAC CRT – Mrs Jo White (MOPAC CRT manager) or in her absence Ms Judith Mullett (MOPAC head of Professional Standards and Workforce)
2. They will complete a report of what the exact breach was and how it occurred and what systems were involved. Additionally it should clearly state what information has been effected and should include specifics as to personal data or special category data. Both organisations should fully cooperate in order to provide all reasonable assistance, information and records to assist with compliance with Data Protection Legislation in respect of the breach.
3. The Information Assurance Unit should be informed as soon as practicable and a copy of the report provided to them.

3.9 Compliance

All partners are responsible for ensuring that appropriate security controls are implemented and staff are aware of their responsibilities under the Data Protection Act 2018.

All partners agree where necessary to allow annual peer-to-peer reviews to ensure compliance with the security section of this DSA. Compliance with these security controls will be catered for in the periodic reviews of this DSA.

3.10 Review

In accordance with the Guidance on the Management of Police Information (MoPI) this DSA will be reviewed six months after implementation and annually thereafter.

Each review will consider the following:

1. Key contacts
It will be important to ensure that each organisation party to the agreement still holds correct contact details for the key personnel operating or managing the data sharing.

2. Usefulness/purpose
All parties will consider whether the information sharing is proving useful, and that the purposes for which it was established are still relevant to the work of the organisations concerned. If the agreement is no longer useful it should be formally terminated.

3. Fit for purpose
All parties will consider whether the information exchanged is fit for purpose. Is the right information being shared at the right time and in the right way? If the data sharing is not working, then the possibility of changing it will be explored.

4. Legal basis
All parties will investigate whether any relevant legislation has been amended, or any new legislation enacted that would impact upon the agreement. If changes have taken place, the agreement may need to be amended to reflect this.

5. Incidents (process)
This will be an opportunity for anyone involved to discuss any problems that have arisen regarding the process of exchanging the information (e.g. has the data been exchanged on time, have there been any complaints about its use etc). It should be noted that complaints about the use of data should not wait until a 6-monthly review. Any complaint should be dealt with immediately

6. Incidents (security)
This will be the opportunity for anyone involved to discuss any security incidents that have occurred (e.g. unauthorised disclosures, physical/IT security failures). Credible assurances should be provided that any failures have been dealt with. Regular failures in security are likely to lead to the termination of the agreement.

7. Renewal/termination
At the conclusion of the Review all parties should either renew the agreement for a further year or terminate it.

Section 4: Legal basis for sharing data

Section 4 of this DSA explores the legality of sharing data. It details how this agreement will comply

4.1 Human Rights - Article 8: The Right to Respect for Private and Family Life, Home and Correspondence

Article 8 says:
(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.

However, this is not an absolute right and when weighed against the public interest, it may be justifiable to interference with this right.

Q29. Show below how this Data Sharing Agreement is:
In pursuit of a legitimate aim: *e.g. preventing or reducing crime – under Statute or Common Law* The sharing of Personal Data with MOPAC for the purposes set out in this Agreement is a Public Interest Task under Article 6(1) (e) of GDPR and with regard to the sharing of Special Category Data it is substantially in the public interest under Article 9 (2) (g) of GDPR and it is substantially in the public interest under national law in relation to criminal convictions as required by Article 10 of GDPR. Relevant national law provisions are detailed below in section 4.2. For the performance of a task carried out in the public interest– Regulatory Requirement. MPS gather the information whilst discharging their duty in the logging, handling and investigating of complaints. MOPAC CRT are required to conduct reviews of these outcomes as provided for under law – Police Crime Act 2017 – Police Complaints and Misconduct Regulations 2020. This is further supported by Home Office statutory guidance and IOPC statutory Guidance. This would constitute a public task. Guidance below as provided by the ICO: You can rely on this lawful basis if you need to process personal data: • ‘in the exercise of official authority’. This covers public functions and powers that are set out in law; or • to perform a specific task in the public interest that is set out in law. (Assessment of Review) • It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.
Proportionate: It is a proportionate means by which MOPAC CRT can discharge their duty as a Relevant Review Body in assessing Reviews of material and outcomes the MPS has gathered in complaint recording and handling.

It is also proportionate for the MPS to meet its legal obligations under the same legislation in providing the required material.

Appropriate and necessary in a democratic society:

It is appropriate to share this information as legislation directs the MPS to share any information that is reasonable for MOPAC CRT to be able to discharge their duty as a Review Body. There is a legal right of review for the public and MOPAC CRT are responsible for meeting that requirement. They can only do that with access to the relevant information held by the MPS. It is also appropriate and necessary for the MPS to comply with their legal obligation to furnish MOPAC with this information.

4.2 Schedule 1, Part 2 Data Protection Act (2018)

In order to process and share Special categories of personal data and criminal convictions data etc, **at least one Substantial Public Interest Condition must be satisfied**.

Q30. Select the condition(s) that apply from the list below and explain why:	
Statutory etc and government purposes Section 6(1)(2). MOPAC are directed by the Police Crime Act 2017 and Police Complaints and Misconduct Regulations 2020. to carry out a function in relation to the data. The MPS are compelled by relevant sections of the same legislation to provide MOPAC with that information.	**Y**
Administration of justice and parliamentary purposes Section 7(a)(b). *Please type here*	**N**
Preventing or detecting unlawful acts Section 10(1)(2)(3). *Please type here*	**N**
Protecting the public against dishonesty etc Section 11(1)(2). *Please type here*	**N**
Regulatory requirements relating to unlawful acts and dishonesty etc Section 12(1)(2). MOPAC will be engaged in the role of reviewing complaint investigations and making subsequent recommendations.	**Y**
Preventing fraud Section 14(1)(2). *Please type here*	**N**
Suspicion of terrorist financing or money laundering Section 15(a)(b). *Please type here*	**N**
Safeguarding of children and of individuals at risk Section 18(1)(2)(3)(4). *Please type here*	**N**

4.3 Schedule 1, Part 3 Data Protection Act (2018)

In order to process and share personal data, **at least one additional condition relating to criminal convictions** in Schedule 1, Part 3 must be satisfied.

Q31. Select the condition(s) that apply from the list below and explain why:	
Consent Section 29. *Please type here*	**N**
Protecting individual's vital interests Section 30(a)(b). *Please type here*	**N**
Personal data in the public domain Section 32. *Please type here*	**N**
Legal claims Section 33(a)(b)(c). *Please type here*	**N**
Judicial acts Section 34.	**Y**
Administration of accounts used in commission of indecency offences involving children Section 35(1)(2)(3)(4). *Please type here*	**N**
Extension of conditions in Part 2 of this Schedule referring to substantial public interest Section 36. *New reform legislation under Police Crime Act 2017 and Police Complaints and Misconduct Regulations make a requirement upon MOPAC to adopt the responsibilities of Relevant Review Body*	**N**

4.4. Schedule 8, Part 3, Data Protect Act (2018)

In order to process and share special category data, **at least one condition relating to Special Category Data** in Schedule 8, Part 3 must be satisfied.

Q32. Select the conditions that apply from the list below and explain why:	
Statutory etc purposes Section 1(a)(b). MOPAC are directed by law to carry out a function in relation to relevant data. The MPS are compelled by law to provide MOPAC with that information.	**Y**
Administration of justice Section 2. *Please type here*	**N**
Protecting individual's vital interests Section 3. *Please type here*	**N**
Safeguarding of children and of individuals at risk Section 4(1)(2)(3)(4). *Please type here*	**N**
Personal data already in the public domain Section 5. *Please type here*	**N**
Legal claims Section 6(a)(b)(c). *Please type here*	**N**
Judicial acts Section 7. *Please type here*	**N**
Preventing fraud Section 8(1)(2). *Please type here*	**N**

Archiving etc Section 9(a)(b)(c). *Please type here*	**N**

4.5. Data Protection Principles

Article 5 of the GDPR stipulates the key responsibilities for organisations in processing Personal and Special Category Data.

Under the GDPR and Data Protection Act (2018), all individuals have rights concerning how their data is used.

- Signatories to this agreement will respond to any notices from the Information Commissioner that impose requirements to cease or change the way in which data is processed.

First Principle

The processing of Personal Data must be lawful, fair and transparent.

This DSA will invoke: the following Statutory Powers: The Police and Crime Act 2017 Parts 1 – 4, and the Police Complaints and Misconduct Regulations 2020 – all sections, in order to share data.

Q33. Explain why you are using this primary legal gateway and what Acts (including the section and subsection) you are relying on:

The reason for the use of these Statutory Powers are: that they are key legislation which set out clearly defined roles and responsibilities which require the sharing of data in order to discharge those duties.

The relevant legislation is:
Police and Crime Act 2017
Police Complaints and Misconduct Regulations 2020 – Regulation 28
Police Reform Act 2002 (as amended by PCA 2017) Part 2.

People should have a legitimate expectation about how their data will be used. Failure to do so, without a lawful basis would be unfair. To help with this, the MPS has produced a Privacy Notice. For more information about this, and where exemptions may apply, please contact the ISSU or visit our intranet site.

Q34. State how you will inform data subjects about the use of their data[4]. If it will not be possible in this case then explain why:

This DSA is about the MPS's processes involved in MOPAC having access to Centurion to conduct their Review.

The MPS discharge this responsibility via its privacy notice which is available online and via the link below:

https://www.met.police.uk/privacy-notice/
-5. Why do we use personal data?
-8. Who will we share data with?

MOPAC discharge this responsibility via its own privacy notice which is also available online and via the link below:
https://www.london.gov.uk/what-we-do/mayors-office-policing-and-crime-mopac/about-mayors-office-policing-and-crime-mopac/mopac-complaints

What we do with your data

Second Principle

Personal Data collected must be specified, explicit and legitimate and must not be processed in a manner that is incompatible with the purpose for which it was collected.

Q35. State how this agreement will comply with the Second Data Protection Principal:

Records marked in Centurion as 'Public Complaint' has been collected from other systems by the MPS, in order for MPS DPS to conduct a Review.

MOPAC CRT's access to the same information held in Centurion is not incompatible with the MPS's purpose. MOPAC CRTs access to Public Complaints is as required in their capacity as RRB.

Third Principle

Personal Data processed must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

[4] You should also mention the normal MPS practice of publishing Data Sharing Agreements on our FoI Publication Scheme so that members of the public can see what is done with their data, unless there is a legitimate reason for not doing so.

Q36. State how this agreement will comply with the Third Data Protection Principal:

The personal data and other information contained in the records marked as 'Public Complaints' are adequate, relevant and not excessive for the Review purpose conducted by MOPAC CRT as a RRB.

Fourth Principle

Personal Data processed for must be accurate and, where necessary, kept up to date.

Q37. State how this agreement will comply with the Fourth Data Protection Principal:
Include what measures are in place to ensure the data shared by the MPS and or the Partner Organisation(s) is accurate and up to date and who is responsible for informing the MPS and or the Partner Organisation(s) of inaccuracies or notifications of new information such as a change of address.

The business of Public Complaint logging, handling and investigating is one which is done on the basis of the information provided by the member of the public. If either the MPS or MOPAC become aware that the details are not up to date, inaccurate or have changed then they will inform the other party as soon as practicable to ensure data is as accurate as possible at all times.

Fifth Principle

Personal Data processed for must be kept for no longer than is necessary for the purpose for which it is processed.

It may be stored for longer periods for research, statistical or archiving purposes in the public interest, subject to the implementation of appropriate measures to safeguard the rights and freedoms of individuals.

Q38. State how this agreement will comply with the Fifth Data Protection Principal:
Include a statement about how long the MPS and or the Partner Organisation(s) will keep the data for.

The MPS complies with its responsibilities under the Management of Police Information (MoPI) in respect of the retention and weeding of data. Most data held by the MPS which would attract a review from MOPAC would be MoPI group 3 (in simple terms retained for 6 years), and in rare cases MoPI group 2 (in simple terms retained for 10 years). In respect of its sharing of data in this instance, MOPAC will access the relevant record and will review the data held therein in order to come to a conclusion and make recommendations. They will not lift the data per se but will refer to it in and quote from it in their findings. It is envisaged that MOPAC will *not* make copies of any documents and there will be no printing of the data. In the event that therer are written notes to aid in the assessment of reviews these will be securely stored and disposed of by means of an approved cross saw shredder.

Sixth Principle

Personal Data processed for must be so processed in a manner that ensures appropriate security of the Personal Data.

This includes the protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures.

Q39. State how this agreement will comply with the Sixth Data Protection Principle:

The MPS employs a dedicated systems administrator to oversee the entire Centurion system. This person is able to add and remove those that require access/no longer require access. There is a specific account set up for each user under a unique user name and password. Alongside this the account profile for the individual will provide only that access that the user is entitled to. In addition to this all users are trained in use of the system and the system has warning signs on logging in. The system is fully auditable. No data will be routinely moved outside of the system.
Security controls in place for MOPAC will be the same as those for the MPS, as users of the system, they will be subject to auditing of their use of Centurion activity in the event that there is evidence of wrongdoing, no documentation will be removed from the secure working environment. No paper copies will be made. All members of the MOPAC CRT have been provided with MPS Laptops and can access the Centurion system via them. These laptops are subject to the same rigorous controls as for MPS personnel.

4.6. Freedom of Information and Right of Access Requests

FOIA Requests: Normal practice will be to make all DSAs externally available on the MPS Publication Scheme. It is recognised that parties to this agreement may receive a request for information made under FOIA that relates to the operation of this agreement. Where applicable, all Partner Organisation(s) will observe the Code of Practice made under Section 45 of the FOIA, relating to consultation with others who are likely to be affected by the disclosure (or non-disclosure) of the data requested. The Code also relates to the process by which one authority may also transfer all or part of a request to another authority if it relates to data held only by the other authority.

Right of Access Requests (GDPR and DPA 2018): Individuals can request a copy of all the data an organisation holds on them, by making a Right of Access request (ROAR). This may include data that was disclosed to that organisation under this agreement. Where this is the case, as a matter of good practice, the organisation will liaise with the originating agency to ensure that the release of the data to the individual will not prejudice any ongoing investigation/proceedings.

DPA 1998 – refers to Rights of data subject & others
GDPR 2016 – refers to Rights of the data subject
DPA 2018 – refers to Rights of the data subject

So the MPS calls them Right of Access Requests instead of the old name SARS – Subject Access Requests

Section 5. Agreement signatures

The Signatory Organisations signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of data between their agencies in a manner compliant with their statutory and professional responsibilities.

As such, they undertake to:

- Implement and adhere to the procedures and structures set out in this agreement.
- Accept responsibility to ensure that all staff involved are trained and fully aware of the procedures and structures of the agreement.
- Ensure that where these procedures are complied with, no restriction will be placed on the sharing of data other than those specified within this agreement.
- Engage in a review of this agreement with partners six months after its implementation and annually thereafter.

We the undersigned agree that each Partner Organisation that we represent will adopt and adhere to this Data Sharing Agreement:

Agency	Post Held	Name	Signature	Date
MPS	**Head of Department**	[redacted]	[redacted]	**19/01/21**
MOPAC	**Head of Department**	[redacted]	[redacted]	**20/01/21**

This DSA was quality assured by the following people in the ISSU:

[redacted] on 22/08/2020, 05/09/2020, and 07/09/2020.
This is now ready for sign off on 07/09/2020.

Sent to [redacted] DPO for Approval & Sign Off 07/09/2020.
[redacted], Information Sharing Lead, satisfied 17/11/2020.