Freedom of Information Act Publication Scheme	
Government Security Classification	[N/A]
Publication Scheme Y/N	[N/A]
Title	A purpose specific Data Sharing Agreement (DSA) between DPS Reviews Team and MOPAC
Version	Version 2.0
Summary	An agreement to formalise data sharing arrangements between the DPS Reviews Team and the MOPAC Police Complaints Reviews Team (CRT), to enable the CRT to perform their statutory duties to scrutinise, support and challenge the MPS regarding their management and/or investigation of complaints from members of the public.
(B)OCU or Unit, Directorate	Directorate of Professional Standards, Reviews Team
Author	[s.40] [redacted]
Review Date	30/07/2020
Date Issued	30/01/2020
ISA Ref	

Purpose Specific

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

Table of Contents

This Data Sharing Agreement is for Law Enforcement purposes only. Under Part 3 of the Data Protection Act (2018), the MPS qualifies as a competent authority for the purposes of: "the prevention, investigation, detection or prosecution of criminal offences; or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."

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 out 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), Law Enforcement Directive and the Data Protection Act (2018);
- 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 signatories to this agreement will represent the following agencies:

- MPS, **Directorate of Professional Standards** (DPS) – Reviews Team and
- **MOPAC** – Police Complaint Review Team

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 '*Appeals*' and which in the future will be known as '*Reviews*'. Further, this agreement accounts for the new responsibilities placed upon MOPAC to record and handle complaints against a Chief Officer of the MPS, and to provide oversight of the complaints system.

The specific legislation is the Police and Crime Act 2017 and the Police Complaints and Misconduct Regulations 2020. These are legislative reforms which move the responsibility for being a Relevant Appeal Body from forces (Metropolitan Police Service) to 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)

In order to accomplish this the MPS will need to provide details of and background papers to public complaints, which contain both types of 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 relevant review body.

In addition to the above, the MPS will need to provide full access to their record management system (currently Centurion), to allow MOPAC to enter information regarding Chief Officer complaints, and to fulfil their role of providing oversight data to the IOPC.

MOPAC shall not share data provided to them by the MPS in support of their role as the review body with the IOPC without prior agreement with the MPS.

Q2. Explain briefly what this project aims to achieve:

The aim of this DSA is to agree a data sharing protocol between the MPS reviews team(who currently conduct force appeals as well as servicing IOPC appeals data requests) and MOPAC.

It is to ensure that the MPS shares information in the most appropriate manner by the most appropriate means in order that MOPAC can discharge their legal obligations.

It is proposed that MOPAC are given access to the MPS DPS Centurion Complaints and Conduct system in order to facilitate the sharing, recording and oversightof information/data , in line with their statutory obligations.

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.

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

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

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 specific data from MOPAC
- MOPAC will use MPS data in order to discharge their legal function as a review body, the body responsible for recording complaints against a Chief Officer, and the body responsible for scutinising, supporting and challenging the overall performance of the MPS complaints process
- MOPAC will return the data with their assessment and recommendations along with the original data.

Q6. Explain the benefits of this sharing agreement for: Centurion

a) The MPS:

- The MPS are legally obliged under the new legislation to provide any information that the review body deems necessary in order for them to discharge their duties. It will allow the MPS to meet this legal requirement whilst ensuring the security of the data and also adherence to DPA principles.

[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.

b) The Partner Organisation(s):

- MOPAC are legally obliged under the new legislation, in certain instances, to take on the role of the relevant review body for public complaints. 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 (non) recording or outcome of that complaint.
- In addition, full access to the Centurion system will allow MOPAC to fulfil their statutory responsibilities regarding the recording and handling of complaints against a Chief Officer, and oversight of the MPS complaints system.

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
- Independent handling of Chief Officer complaints
- Independent oversight of the MPS complaints system.

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.*

- Centurion – full access, aside from data withheld, or stored as “SECRET” or “TOP SECRET” according to government security classifications
- CRIS – Name, Address, dob, gender, ethnicity, dets of investigation, VIW, Susp
- CrimInt - (subject to harm test) relevant extract dets
- Merlin - (subject to harm test) relevant extract from dets
- CAD – All fields
- IIP – 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 to facilitate the provision of any relevant information or data which will enable MOPAC to discharge their duty as a relevant review body and oversight body.

Q9. Please confirm the following:

MOPAC will not disclose MPS data shared under the terms of this agreement with a third party without first seeking the permission of the MPS unit that provided it. Including any interested party.

Yes - clarification – the unit that supplied the data (PSU or DPS) will decide, any such request should be in writing (including via secure email) and should be replied to formally by the same means.

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 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, Law Enforcement Directive legislation, 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 will seek the explicit[2] consent of its data subjects:

No

If the answer if no, please explain why:

MOPAC will be the relevant review body whose role and responsibility will be to conduct reviews that they receive from members of the public into the (non)recording and outcome of complaints that they have made. Therefore it follows that they will already be aware of the personal data that they have shared with the MPS in the first place and the purpose of that.

If the answer is yes, explain how explicit consent will be sought, providing evidence if applicable: *i.e. attach a copy of the consent form you used to the appendix of this DSA or provide the wording given to data subjects in order to obtain their consent.*

A note will be added to outcome letters/reports which, when advising of the right of Review, and will state**: Any personal data submitted in the course of making a complaint will be processed and used to provide an outcome to that complaint. Any right to Review will mean that the MPS**

[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.

will provided that data to the Relevant Review Body in order that they can conduct the review

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:

It is proposed that MOPAC will inform the public that their personal data is to be used in order to conduct the complaint review at the point of first contact when confirming receipt of the review application.
This will be achieved in two ways, firstly with the statement in bold in Q12. Above, and then also by a similar statement by MOPAC when they make initial contact with the complainant.

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 compelling reason for sharing data with the partner organisation is so that they can conduct complaint reviews on request of the public. MPS will provide a warning that will be printed with every right of Review. It will advise the public that the MPS will share their personal data with the Review Body in the event that they exercise their right of review. MOPAC will have a duty to not disclose the data beyond the third party or interested parties unless explicit agreement is obtained from the MPS.

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 will make requests for review relevant data in writing to the MPS DPS Reviews Team. MOPAC will not need to request specific data from the MPS for oversight analysis work to be conducted, but will advise the MPS when outcomes are available from the assessment of data.

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

The MOPAC Public Complaints Review Team 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:

Initial requests for data will be made via email and then subsequently can be by phone or via centurion workflow.

Q16. How will the MPS gather the data requested?

The MPS will gather data during the course of a complaint investigation. It gets recorded onto Centurion under unique references relating to each individual case. If there is a requirement for further material that is not attached to the Centurion record then this will be requested by the DPS via email to thethe relevant Professional Standards Unit.

The initial complaint containing personal data would be received in the MPS in a variety of ways, online, in person, via the IOPC etc. The MPS officer appointed to conduct a complaint investigation will likely generate, review or obtain documents, which include personal and special category data. This is stored locally (BCU S Drive). If MOPAC request background papers to conduct a review, documents containing that data will be provided to the DPS for storage on Centurion and the DPS S drive, to then be forwarded to and/or accessed by MOPAC to complete a review.

Who will be responsible for doing this?

The MPS DPS Reviews Team will initially be responsible for completing these data requests. MOPAC will interrogate Centurion independently for oversight functions and to perform their role to provide feedback to the IOPC.

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

- [redacted] Head of Workforce and Professional Standards (Police Staff Seconded to MOPAC)

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

- MOPAC Police Complaint Review Team

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

- [redacted] MOPAC Project 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 will require actual access to Centurion. This is the national complaints and conduct system, which is restricted to DPS personnel only. The MPS will provide full access of Centurion to MOPAC, to enable them to fulfil their statutory responsibilities This will allow a case to be reviewed in its entirety along with attached documents (where they have actually been attached and not stored locally) to any recipient/group, which is set up on the system. Within MOPAC, the access would be limited to the MOPAC Police Complaint Reviews Team and wider Professional Standards Team (for resilience purposes). This is a total of ten people.

[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)?

If the MPS requires data from the MOPAC Review Team then it would be requested in writing.

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

Requests would be made by the MPS Reviews Team.

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

Requests will be made via MOPAC, government rated secure email or by means of using the workflow system within Centurion. In exceptional circumstances, it may be that a request is made by phone or in person, as the MOPAC team will be co-located within the MPS Reviews Team.

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

MOPAC will collate data on the Centurion system and add relevant documents to the document section as they progress their review assessments, and when a complaint is received about the Chief Officer.

b) Who will be responsible for doing this?

Members of the MOPAC Police Complaints Review Team will be responsible for gathering and collating this material, with the assistance of the MPS DPS Reviews Team.

c) Which systems will be interrogated?

Only Centurion and any documents and background papers attached to an individual record will be interrogated in order for them to collate their complaint reviews. All Centurion data may be analysed for oversight purposes.

It may be that MOPAC receive further information from the complainant, that was not initially disclosed during the initial complaint process and this may require MOPAC to make secondary requests for data such as extracts from CRIS, CAD etc.

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

- [redacted] Head of Workforce and Professional Standards [redacted]

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

- The MPS DPS Reviews Team.

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

- **There is no secondary point of contact at MOPAC at this time**

The **MPS SPOC – MPS Reviews Team,** will create a record of any personal data disclosed to **MOPAC** on Centurion, 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.

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" (unless there are national security implications, in which case a Counter Terrorist Check (CTC) is required). **MOPAC** must confirm that employees who will access shared data will have a genuine "need-to-know", and that they have provisions in place to ensure that unauthorised dissemination or copying by their staff 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 all of the staff that will constitute the MOPAC Police Complaint Review Team will be SC vetted. This will be necessary in any case as they wish to co-locate within the DPS footprint which requires this level of vetting as a condition of entry.

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 Police Complaints Review Team will be subject to vetting to the same level as MPS users of the Centurion system. It may be that there is a confidentiality requirement within their contract of employment.

3.3 Data Transfer

Hard Copy

Hard copy documents would be passed by means of sealed envelope by a member of the MPS Reviews Team to the MOPAC police complaints review team. As both teams are to be co-located this method of transfer is unlikely.

Electronically

- Data marked with a Government Security Classification up to the level of OFFICIAL SENSITIVE will be transferred using either Centurion workflow or secure government email. 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:
i.e. in a locked container within a secure premise with managed access controls, such as swipe, pin or key entry. If this does not apply state that the Partner Organisation(s) will not use hard copies of the shared data.

MOPAC will store their findings and recommendations on the Centurion system. Should they have the need to make additional records they will be stored on the MOPAC servers, which are government security rated. Additionally, any paper copies will be stored in the appropriate secure locking cabinets behind a locked door within their designated work area of ESB. All access doors within the DPS footprint are access controlled.

Electronically on a Partner's system

Q25. Explain what system access controls the Partner Organisation(s) has in place to keep MPS information safe:

MOPAC will be subject to the same system controls that are employed by the MPS and they include: user name, password, access limited to only the seven members of the Review Team, plus the additional three members of the wider MOPAC professional Standards Team, which is a need to know basis. MOPAC will not access any MPS owned information beyond the duration of the time necessary for assessment and oversight purposes.

Q26. MOPAC confirm that the MPS data they hold can be audited at any time.

Yes – MOPAC will use an MPS system which is fully auditable. If the answer is no please state why: n/a
Q27. MOPAC is part of the UK Government Cyber Essentials scheme. MOPAC 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 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.

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 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

- Papers will be disposed of using a cross shredder.

Electronic Information from Partner's System

- Electronic data held on a Partner Organisation's system will be securely erased or overwritten using an approved software utility to a standard applicable to the Government Security Classification.

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 **Detective Superintendent – Head of RIU** without undue delay of occurring/or no later than 24 hours after the Partner Organisation(s) 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 [s.40] 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 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 24 hours, the unit discovering the breach would inform the senior member of the MOPAC Review Team.
2. They would 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
3. The Information Assurance Unit should be informed and a copy of the report provided to them.

3.9 Compliance

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

All partners agree where necessary to allow 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.

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* Legitimate policing purpose – Regulatory Requirement. MPS gather the information whilst discharging their duty in the logging, handling and investigating of complaints. MOPAC 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. These legislative and national guidance documents also require MOPAC to maintain oversight of the MPS complaints process.
Proportionate: It is a proportionate means by which MOPAC can discharge their duty as a relevant appeal body in assessing Reviews of material and outcomes the MPS has gathered in complaint recording and handling.
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 to be able to discharge their duty as an appeal body. There is a legal right of review for the public and MOPAC are responsible for meeting that requirement. They can only do that with access to the relevant information held by the MPS.

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

In order to process and share personal data, **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 law to carry out a function in relation to the data. The MPS are compelled by law 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 outcomes 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. *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.*	**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. *Please type here*	**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 the 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.
- The MPS reserves the right to withdraw the use of this data at any time.

First Principle

The processing of Personal Data for a Law Enforcement Purpose must be lawful and fair.

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.

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:

Data subjects submit their personal data to the MPS in order to lodge a public complaint. They may provide further information or data in order that a compliaint investigation can take place. On conclusion, they are provided an outcome. They can if they choose exercise their right of review if they disagree with the outcome. They will therefore already be aware of what they have supplied, what it will be used for, and how it will be used. A privacy notice will be added to all correspondence where a right of review exists. This will explain that the data they provided in submission of their complaint will be shared with the relevant Review Body for the purpose of that body to conduct a review if they choose to exercise their right in this respect.

Second Principle

Personal Data collected for a Law Enforcement Purpose 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:

Compliance with the second principle will be met by ensuring that MOPAC will have to provide evidence of a request for review to the DPS, prior to attempting access to a specific Centurion record. A copy of this request will be added to the case progress log (this provides a running log of activity) and thus will demonstrate the explicit, specific and legitimate purpose for the processing of the data. MPS must remind MOPAC that the data can only be used for the purpose intended when providing it, and in accordance with the statutory responsibilities placed upon MOPAC.

Third Principle

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

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

The personal data collected for the original complaint logging, handling and investigating is done so in order to discharge the legal duty in this respect. This Data Sharing agreement is an extension of that responsibility in that MOPAC require access to that information in order to conduct reviews when in receipt of applications to Review specific complaints.

Fourth Principle

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

[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.

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 at the first available opportunity to ensure data is as accurate as possible at all times, and ensure the data is corrected on Centurion.

Fifth Principle

Personal Data processed for a Law Enforcement Purpose 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 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 level 1, and in rare cases MOPI level 2. In respect of its sharing of data in this instance, MOPAC will access the relevant record once supplied 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 their findings. It is envisaged that MOPAC will *not* make copies and in the event that they do, they will be destroyed by means of an appropriate cross saw shredder of government approved standard, once the review is complete.

Sixth Principle

Personal Data processed for a Law Enforcement Purpose 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 Principal:

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 and subject to regular checks. 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, no documentation removed from the secure working environment. Any required paper copies to be kept in a lockable container behind a locked door.

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.

- The Signatories of this agreement will comply with right of access requests in compliance with the relevant legislation (GDPR/DPA 2018), and if it is to be answered jointly, to inform the MPS as soon as possible on receipt in order to comply with the statutory time limit.

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]		
MOPAC	**Head of Workforce and Professional Standards**	[redacted]		

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

[Insert Name] on **[Insert date]** and **[Insert Name]** on **[Insert date]** and signed off on **[Insert date]**.

The ISSU now confirm that this DSA is DPA (2018) compliant and you can now proceed to obtain wet signatures and general registry file number. Please send the ISSU a scanned copy of the signed agreement for our records.

Appendix A

Data Protection Principals

First Principal
The processing of personal data for a law enforcement purpose must be lawful and fair.

The ICO website says the following:
You need to be aware that any processing you carry out for the law enforcement purposes must be necessary. In practice, the lawful basis would either be necessary for the performance of a task carried out for law enforcement purposes by a competent authority, or based on consent. There may be circumstances where you obtain consent from the individual whose data you are processing, although this may only be appropriate in certain circumstances. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means.

- Lawful (processing) - means that you are authorised by either statute, common law or royal prerogative, or by or under any other rule of law.
- Fair - requires you to be, where appropriate, clear and open with individuals about how you use their information, in keeping with their reasonable expectations.

When processing Special Category Data:
You must be able to demonstrate that the processing is **strictly necessary** and satisfies one of the conditions in Schedule 8 or is based on consent. Strictly necessary in this context means that the processing has to relate to a pressing social need, and you cannot reasonably achieve it through less intrusive means. This is a requirement, which will not be met if you can achieve the purpose by some other reasonable means.

Second Principal
Personal data collected for a Law Enforcement purpose 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.

The ICO website says the following:
Any processing under Part 3 of the Act must be for the defined law enforcement purposes. You cannot process for a purpose that is incompatible with the original reason and justification for processing.

Third Principal
Personal data collected for a Law Enforcement Purpose must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

The ICO website says the following:
The third principle requires that the personal data you are holding is **adequate** and **limited to** what is necessary for the purpose(s) you are processing it.

Fourth Principal
Personal data processed for a Law Enforcement Purpose must be accurate and where necessary, kept up to date.

The ICO website says the following:
The fourth data protection principle is about accuracy. It sets out that you should take every reasonable step to correct inaccurate data. In addition, **as far as possible**, you need to be able to distinguish between personal data that is based on factual data and that which is based on a matter of opinion or assessment, such as a witness statement.

A new requirement is that again, where relevant, and as far as possible, you need to be able to distinguish data between different categories of individuals, such as suspects; individuals who have been convicted; victims and witnesses. You only categorise information under Part 3 that is relevant to your investigation, and other unused data falls under the general provisions of GDPR and Part 2 of the Act.

Fifth Principal
Personal data processed for a Law Enforcement Purpose must be kept for no longer than is necessary for the purpose for which it is processed.

The ICO website says the following:
The fifth principle requires that you do not keep personal data for longer than is necessary for the purpose you originally collected it for. No specific time periods are given but you need to conduct regular reviews to ensure that you are not storing for longer than necessary for the law enforcement purposes.

Sixth Principal
Personal data processed for a Law Enforcement Purpose must be so processed in a manner that ensures appropriate security of the personal data.

The ICO website says the following:
The sixth principle requires you to have technical and organisational measures in place to ensure that you protect data with an appropriate level of security. This is the same as under GDPR and Part 2 of the Act.

'Appropriate security' includes 'protection against unauthorised or unlawful processing and against accidental loss, destruction or damage'.

Appendix B

Evidence of Consent

Please attach here a copy of the consent form you will use.