



Data Protection Impact Assessment (DPIA)

DPIA Information	
Date Received	14/09/2026
Name (and or project number)	Forces Use of Copilot – Artificial Intelligence (AI)
Forces involved in Project	Joint
Business Area/s Affected	Forcewide
Force SIRO	[REDACTED]
Information Governance Contact	[REDACTED]
Freedom Of Information:	Yes, this document will be public facing with anonymisation of signatory details only.

Template Review Information			
Version History	Version Date	Requestor of Change	Summary of Change(s)
1.0	24/05/2018	Regional Feedback	Agreed final version
2.0	02/09/2024	Audit Feedback	Updates to format
2.1	26/05/2026	Fol	Comment added for Fol approval
2.2	05/08/2026	Stakeholder Feedback	Minor Language Changes

Guidance Document:

The below link provides the supporting documentation, if required.

- [Find out about Data Protection Impact Assessments \(shdc.police.uk\)](https://shdc.police.uk)

Introduction

The **Data Protection Impact Assessment (DPIA)** process is an important tool to help you identify and minimise the data protection risks of a project that involves processing personal data.

The DPIA process is relevant to initiatives involving the use of personal data and is particularly important when a new business process or technology initiative involves the collection, recording, sharing or retention of personal data.

The DPIA enables privacy and data protection considerations to be made in the early stages of a project where any identified problems can be easier to resolve rather than late or retrospective consideration where solutions can be more costly or delay implementation. A DPIA, can also identify whether the project should be continued when balanced with the rights and interests of persons affected.

The DPIA process will consider privacy in the way the forces use individual's personal data. This can involve privacy about: the integrity of the individual, the person, their personal information, their personal behaviour and their personal communications.

When carried out early the DPIA process can provide the following benefits:

- identify any privacy or information risks concerning the processing of personal data
- determine any mitigations necessary to bring those risks down to an acceptable level
- provide a record of those mitigations and the decision by Business Lead whether to accept and adopt them
- provide a record of the Data Protection Officer's views on the initiative.

Who is responsible for carrying out a DPIA?

The Project Manager will be responsible for ensuring that the DPIA is completed. In the absence of a Project Manager it will be the relevant specified Business Lead. The Information Governance team will assist you and explain how the DPIA should be completed.

The DPIA will require authorisation by:

- Information Asset Owner and Senior Responsible Officer
- Information Governance team or the Data Protection Officer
- Senior Information Risk Officer – where the DPIA has identified 'high' residual risks and referral to the Information Commissioner is require

Freedom of Information Act (FOIA) & Information Security

This document (including attachments and appendices) may be subject to an FOI request. If requested, Sections 1 and 4 will be considered under the FOIA with relevant redactions where necessary. Please advise the Information Management team in advance if you require specific exemptions applied.

In compliance with the [Government's Security Policy Framework's \(SPF\)](#) mandatory requirements, please ensure any onsite printing is supervised, and storage and security of papers are in compliance with the SPF. Dissemination or further distribution of this document is strictly on a need-to-know basis and in compliance with other security controls and legislative obligations.

1. Outline of the project, objectives and benefits

The purpose of this DPIA is to review Sussex Police and Surrey Police (hereafter referred to as The Forces) use of Copilot. The Forces have restricted use of Artificial Intelligence (AI) 'chat' functions to Copilot only, as using a single platform like ensures consistency across the organisation, simplifies integration with existing tools and makes governance and security easier to manage. This DPIA will not address processing using AI in other bespoke systems, they are subject to their own specific DPIA.

This DPIA will be published on the Forces external websites for transparency purposes and to assure the Public of the precautionary steps taken to protect their data.

Decisions around the use of Copilot is supported by the National Police Chiefs Council (NPCC) Copilot DPIA which has been reviewed. Processing in Copilot is also supported by the [Forces AI Policy](#).

This is the first iteration of a Copilot DPIA due to legacy governance assurances and restrictions which identified the processing as low risk (no personal data permitted in Copilot). However, as the Forces understand Copilot and have applied processing restrictions, it is necessary for the DPIA to be completed.

The Forces have recently expanded business use cases in Copilot to include limited personal and law enforcement data (there should be no processing of special or sensitive category data in Copilot). Approved use cases will be outlined in [Force Guidance](#) and this DPIA will record the lawful processing of personal (UK GDPR) and Law Enforcement (Part 3 of the UK Data Protection Act), hereafter referred to as Data Protection legislation.

There is a national DPIA available from the NPCC which makes is clear that it is not envisaged that Copilot will be used for personal or operational data. Any significant deviation which makes our forces outliers from this position will require careful rationale and risk assessment. The NPCC also advise that, 'where there are specific purposes that involve special category data, sensitive processing or types of activity that may present a high risk to the rights and freedoms of data subjects, then a separate DPIA is likely to be required'.

In summary, the NPCC itself does not envisage standardised or routine processing of personal/ law enforcement data in Copilot. As regards the use of AI in evidential material, the NPCC has set out a very clear position, 'Generative AI is not authorised for use in the Criminal Justice system for the creation of evidential materials. This means it must not be used in the preparation of witness statements, MG forms, or any other evidential reports'. The Forces will continue to engage with partner agencies, including the Crown Prosecution Service (CPS) to define AI use cases to support law enforcement processing.

Security measures have been implemented to support privacy by design and are necessary to protect the personal data of both the public and staff. In support of this, the Forces have currently restricted any processing of identifiable law enforcement data within Copilot, this includes but is not limited to summarising Occurrence Enquiry Log (OEL) text, writing officer statements, etc. For transparency, this is also under review and any changes will be updated in this DPIA.

The Forces have also deployed Data Loss Prevention (DLP). This is an auditing tool that identifies when a user has breached Force Policy by processing personal or law enforcement data in Copilot. This is actively monitored and repeat cases will be escalated within the organisation. DLP policies are currently being refined to reduce the number of false positives, especially as the Force is reviewing what data is permissible in Copilot.

Information Security have risk assured Copilot which has also been Nationally approved to process Official classification information. However, as stated previously, the Forces have taken additional restrictive steps when using Copilot for the data we process. This should support data minimisation principles and build trust with the public regarding police processing of their data.

For ease of reading, the below bullet points relate to processing of personal, special / sensitive and law enforcement data in Copilot:

- **Anonymised:** This data contains no identifying personal data, such as aggregated statistics, guidance materials, legislative research, etc. This is low risk and permitted within the Copilot infrastructure. There are no perceived risks with this type of data and as such, it is accepted under the Forces tolerance levels and processing of this data is approved

- **Pseudonymised:** This is where additional information would be required to associate data to a living person, similar to a lock and key scenario. This could be using a Niche ID as the identifier along with offending history. Without access to the system, there is no way to identify the nominal. This is considered medium risk dependant on the actual data being entered. This type of processing will be subject to a risk assessment by the user.
- **Personal Data:** The Forces have approved the processing of staff / officer names within Copilot. This is because of the restrictions in place through our Microsoft licence and is further supported by the deactivation of Web Grounding. Public names may be processed through the use of the Outlook settings to review / summarise emails. This will require initial review by the email owner to ensure the data within does not breach other Force processing restrictions. The Forces have not approved the bulk processing of public personal information, restrictions remain in place to protect this data as it falls under Part 3 Data Protection Act.
- **Law Enforcement Data:** The processing of this data is not currently approved in Copilot. The only exceptions being where the data is either anonymised or pseudonymised.
- **Web Grounding:** The Force has turned off web grounding, so Copilot no longer sends information to the internet when generating responses. Instead, it only relies on data already available within the Force network or as updated in the core Microsoft AI. All data processed by the Forces therefore stays inside Microsoft's secure environment, ensuring nothing leaves the Microsoft boundary and that privacy and security for all personal data is maintained.
- **Access To Documents:** Copilot does not have access to organisational content such as files, emails, or chats unless this is explicitly provided by the user in a prompt. Users can share organisational content by including it in their prompt text, attaching a file to their prompt or using an agent that has access to organisational data.
- **Copilot Agents:** Agents in Copilot are AI assistants designed to help users solve problems and complete workflows. They provide deeper integration with specific grounding data compared to general-purpose chat, making them more effective for targeted tasks. Agents will undergo a separate risk assessment before approval by the Forces.
- **Data Encryption in Microsoft Copilot:** Copilot is built on the Microsoft 365 platform and inherits its robust security and compliance capabilities, including comprehensive data encryption measures. These are critical to ensuring that all data processed by Copilot is protected against unauthorised access and tampering.
- **Automated Processing:** This is permitted if the data falls within the approved categories identified above. Automated processing simply means using Copilot to perform an action on large data sets, there will be no automated decision making for law enforcement data.
- **Automated Decision Making:** The Forces do not permit any form of automated decision making when using Copilot. This restriction is enforced through Policy, guidance and training.
- **Human Review and Accountability:** All outputs generated using Copilot will be subject to human review. This is a necessity to ensure both accuracy and ownership of the data. This makes users personally responsible for reviewing the output to ensure it is factual and does not contain hallucinations.
- **Handling Conditions:** All Copilot generated data will carry handling conditions stating its origin. The reason for this is to identify the origin of the output and to clarify for any further processing that the data was created using AI.

The data processed by Copilot will be stored on other police systems, such as Niche, Outlook, SharePoint, etc. Each of these systems has its own governance measures in place, including access levels, retention. To reiterate the above, currently is no processing of law enforcement information in Copilot, however it will be used to process data captured for a law enforcement purposes (with anonymisation or pseudonymisation applied).

Copilot can be used for a number of different reasons and as such advice on specific processing can be obtained from the users respective Information Management teams as and when required.

The approved processing list at the end of the DPIA details the current approved processing at the time of writing. New processing will continue to be reviewed on a case-by-case basis, this DPIA will be updated to reflect these decisions and replicated into the Forces training materials. All of which will be updated online to ensure full transparency with the public.

Copilot sits within the Forces existing Microsoft tenant and as such, it has been confirmed that it will not retain any data used in prompts, will not use any data for machine learning and that all information will continue to be processed within the UK. This, added to the web grounding decisions and current National policing contract with Microsoft offers the necessary assurances for limited processing of personal and law enforcement data.

Consultation:

The Forces have intentionally adopted a cautious approach to the use of its data within Copilot. This is necessary to ensure data sets were fully reviewed and assessed and that we adopt a secure and transparent approach, especially due to the sensitive nature of the information we process.

This decision will remain under constant review. To date, decisions have been reached regarding the relaxing of information we process under the UK GDPR including staff details (not personal information relation to Missing Persons). However, at the time of writing, restrictions remain in place for law enforcement data. This decision has been discussed at length between the DPO and SIRO.

Any decisions to further process law enforcement data will be done in consultation with the attendees of the AI Governance Board and will have final approval from the DPO and SIRO. These will be documented and recorded on this DPIA for transparency.

A strong foundation to protect the public's data, privacy by design and transparency of processing decisions are at the forefront of any decisions.

Data protection compliance – assessment of necessity and proportionality of personal data processing.

Principle 1: Use of personal data is fair and lawful

Copilot is a tool to improve efficiency and where utilised correctly, accuracy. The data processed in Copilot could fall under either the UK GDPR (staffing related and Missing Persons) or Part 3 of the Data Protection Act (law enforcement purposes). It is therefore expected that the processing could fall under multiple lawful basis under both legislative requirements. As Copilot will primarily be used to re-process data, it is important to note that the applicable lawful basis will have been detailed in the original system / point of capture.

There is no 'necessity' associated with the use of Copilot, it is an expediency and efficiency tool. However, our requirements for processing the data in the first place is detailed in the Privacy Notice, Record of Processing Activities and Appropriate Policy documents which are all public facing.

For example, if Copilot is being used to review and summarise meeting transcripts, the purpose of the meeting will have its own governance approval / requirements which detail why the information is being discussed. The use of Copilot will be assessed as lawful if it follows the pre-approved Force guidance on its usage.

Whilst processing of law enforcement and special / sensitive data is not permitted (other than on a case by case basis), the tools in Copilot make this very difficult for the user to foresee. For example, the 'summarise' button in Outlook does not clearly identify that they will be using Copilot to summarise the email thread.

As the user is opting to use this button, rather than reviewing manually, they must accept the risk and potential breach if law enforcement / special / sensitive category data is contained within. This also applies to summarising Teams minutes, briefings, etc. The user needs to be aware and if they suspect the data contains these categories, it is their responsibility to manually redact prior to Copilot ingestion.

This is a necessary distinction to make as Copilot alone does not determine the lawfulness of the processing, it relies on Force governance for existing systems being in place. Therefore, the below are potential lawful basis for the use of Copilot, depending on the user cases that could exist across both the UK GDPR and Part 3 Data Protection Act (note that Copilot will not be used in relation to Missing Persons and therefore no consideration for Vital Interest processing):

- **Personal Data (Article 6 (1) of the UK GDPR):**

- (b) **Contract:** processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (e) **Public task:** processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) **Legitimate interests:** this relates to purely People Services related matters where contract is not relevant. Processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

- **Special Category Data (Article 9 (2) of the UK GDPR):**

- (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- (g) processing is necessary for reasons of substantial public interest (see below for the potential conditions), on the basis of Domestic Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
 - Statutory and government purposes
 - Racial and ethnic diversity at senior levels
 - Preventing or detecting unlawful acts
 - Protecting the public
 - Support for individuals with a particular disability or medical condition
 - Safeguarding of children and individuals at risk
 - Safeguarding of economic well-being of certain individuals
 - Insurance
 - Occupational pensions

- **Lawful basis for processing sensitive data for law enforcement purposes:**

The Forces may process Personal / Sensitive Data under their statutory functions and where processing is necessary for the performance of a task carried out for that purpose by a competent authority. The definition of statutory function for 'law enforcement purposes' is '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.

In addition, the police may process sensitive data where the processing is strictly necessary for the law enforcement purpose and the processing meets at least one of the conditions in Schedule 8, Part 3 DPA 2018 namely:

- Judicial and statutory purposes/administration of justice; the sensitive processing must be necessary for the administration of justice, or the exercise of a function conferred 'on a person' by enactment. This covers a constable and other competent authorities. In addition, in order to satisfy this condition, you must be able to demonstrate that the processing is necessary for reasons of substantial public interest.
- Safeguarding of children and of individuals at risk; this condition is met in cases where consent is not appropriate because the individual is under 18 or at risk, but the processing is necessary for reasons of substantial public interest, and is to protect them from harm or to protect their well-being.

Processing for these purposes is supported by core systems Data Protection Impact Assessments (DPIA), the Forces Privacy Notice, Record of Processing Activities and Appropriate policy documents for Law Enforcement processing.

The Information Commissioner's Office (ICO) defines "strictly necessary" in the context of special / sensitive category data as a targeted, proportionate, and non-routine measure where the specific purpose cannot be reasonably achieved by less intrusive means or by using ordinary non-sensitive personal data. For this reason, Forces have restricted the routine inputting of this data into Copilot. However, there may be exceptions where this is necessary and this will be for the user to assess and record for audit purposes.

Approval to process this type of data will only be given when it is considered strictly necessary because the information is required to support a specific and identified law enforcement purpose and the objective cannot be achieved effectively or accurately without access to that data. Force guidance restricts the processing of this data for convenience, efficiency or expediency alone.

Therefore users must adhere to Force guidance and remove special / sensitive category data unless it is individually assessed as necessary. Where possible, the data must be anonymised or pseudonymised to ensure protection of data subjects personal data and compliance with their Human Rights.

Principle 2: Use of personal data is for a specified, explicit and legitimate purpose and not re-used for a purpose that is in-compatible with the original purpose:

The processing is considered compatible as it is a continuation of the UK GDPR or Part 3 DPA requirements. For example, Copilot may be asked to review Teams transcripts to identify staff issues or to review letters sent from a member of the public to identify repeat concerns. The use of Copilot as a tool does not make the processing incompatible, it is merely an expediency and accuracy mechanism to support the processing of the data and the compliance with the original purpose. It is also only used where deemed relevant or necessary by the user, it should not be the default for all Force processing.

Principle 3: Use of personal data is adequate, relevant and no more than necessary:

The Forces have restricted what data is permitted in Copilot to ensure compliance. The data was initially restricted to only anonymised / non law enforcement identifiable data. As Copilot has developed through Microsoft products, there have been requirements to review these restrictions with the intention of expanding our usage in a lawful and controlled manner.

This is the reason the DPIA is being written now, as the processing in Copilot is no longer considered low risk. However, guidance is clear that Copilot is not a necessity, it is a tool to support expediency. Also, staff / officers must ensure they review the data for necessity prior to any usage of Copilot.

Current approval applied for personal data include staff / officer / corporate (Pay / Warrant / FIN / Email) information and for certain departments, names / emails of suppliers. Consideration is given at the end of this DPIA for the inclusion of public name / email contact and email content, mainly due to the use of the 'Summarise' button in Outlook. Prior to any use of this for public correspondence, the Forces will publish this decision to ensure compliance with the transparency principles.

Principle 4: Personal data must be accurate and kept up to date:

Copilot is dependent on the user assessing the relevance, accuracy and timeliness of the data prior to processing. As stated previously, Copilot is predominantly an expediency tool and it will not replace current / existing Force practices. As part of these current practices, the officer / staff is responsible for ensuring the outputted data is compliant with accuracy prior to making any decisions.

The use of Copilot does not reduce expectations or ownership of the data, the requirement for human review prior to and following any processing remain paramount. Staff are also aware that any outputs generated through Copilot are their responsibility and they own it and any inaccuracies.

These expectations are made clear to staff / officers in the Force guidance. Copilot can be susceptible to error, bias and hallucination which is why its outputs should always be independently checked and not treated as a primary source of truth. It does not replace the necessity for human review and for our staff / officers to fully review, verify and fact check all outputs. Therefore the 4th Principle will ONLY be satisfied when every Copilot output has a proper human review.

Depending on the use case and product produced through Copilot, retention will be applied as per Force Retention Schedule or Management of Police Information (MoPI).

Principle 5: Personal data must be kept in an identifiable format for no longer than necessary:

The 'source data' (i.e. data in the existing Force systems) will be retained as per the retention schedule / MoPI within that system. Any generated using Copilot will also be bound by these restrictions and stored in Force systems. The Force publishes its Retention Schedule on the Internet and any data types we process, irrelevant of origin, will be stored securely under the respective category. This will ensure data is not retained indefinitely and that it is accessible for any review or Subject Rights requests (see point 7 below).

Any law enforcement documentation that is generated using Copilot will be clearly marked with handling conditions. These will ensure full transparency throughout the life of the data to identify that Copilot was used to support its creation.

Copilot prompt data will be temporarily stored under the user settings, similar to Teams Chat settings. These are auto-weeded as per the Force policy for SharePoint / Teams. Copilot does not retain the data it produces for the user, once the request has been actioned and the text extracted / copied, the response is deleted.

Principle 6: Personal data must be protected against unauthorised / unlawful use, accidental loss, damage or destruction:

With regards the Copilot software, this resides on the Forces secure tenant and has therefore undergone the necessary approvals and Information Security risk assessments. The removal of web access has added further protections to the data we process.

Copilot is replacing a current manual process for expediency and efficiency purposes, this will not impact the storage of the data in Force systems.

7. Personal data will be processed in accordance with the individual's data protection rights:

There are existing and established routes for the public to exercise their rights under the legislation. These rights include all data we hold on an individual and will therefore include any materials processed using Copilot. In support of this, and to ensure distinction of AI generated documents, Force users are advised to enter handling conditions stating that Copilot was used in the creation of any documents.

The Right to Be Informed is being met through the external publication of Force documents, including the DPIA and staff learning materials.

Rights Of Access will be managed through the respective Information Access Teams and applications can be made through the Forces website or through any other lawful means. Rights To Rectification / Forgotten are also processed through the Force Internet sites for applications and will be managed by the respective Forces Information Management teams.

Rights of Restriction will be reviewed as per the above Rectification / Forgotten requests. These could be more frequent challenging the use of Copilot for accuracy. However, as stated all documentation and outputs will be reviewed by the human entering the prompts and they are fully accountable for the decisions around accuracy.

8. Personal data will not be transferred outside the European Economic Area (EEA) without guaranteed adequate privacy protections:

Data produced by and processed within the Forces will not routinely be shared outside of the EEA. It will be shared within the UK and Police Forces however, due to the nature of the information we process, there may be requirements on a case-by-case basis to share outside of the UK.

Our current web grounding settings also ensure that data entered in Copilot is not routinely shared on the internet, this setting supports UK only processing.

The issue of International Transfers is discussed within Part 2 of Microsoft's Guide to Generative AI which refers to transfers being lawful if based on an adequacy decision by the European Commission. This is repealed in UK law by the 2025 Data (Use and Access) Act which revises the DPA18. Whilst the intention of the revised legislation is to make international transfers more flexible, the conditions set out are of vital importance where the data being processed is Law Enforcement Data:

- 2- The First Condition is that the international transfer must be NECESSARY for a law enforcement purpose. 'Necessary' cannot be interpreted to mean, 'convenient'.
- 2- A new test created under s74AB DPA18 is that the recipient of data in any third country must be a comparable competent authority and comply with certain standards. Law enforcement data must only be shared internationally with law enforcement agencies who can demonstrate standards comparable with the UK.

MS states that, 'there are limited exceptions to the EU Data Boundary that may result in Microsoft processing Customer Data (including personal data) outside of the EU Data Boundary. Where this is the case, Microsoft relies on complaint data transfer mechanisms as set out in the GDPR'. By GDPR, MS mean the EU GDPR, not the revised UK version. The adequacy provisions of the EU GDPR do not cover UK law enforcement processing.

This creates a risk of overseas processing of law enforcement data which may be lawful under the EU GDPR but would not have a clear lawful basis under DPA18.

Microsoft, like all US-based companies, may conceivably be asked to disclose UK-based data to the US government under their domestic legislation. Further, MS accepted in a communication to Police Scotland in 2023 that data 'can go outside the UK' and that it cannot guarantee data sovereignty.

The risk from unauthorised international transfers is common to all MS cloud-based products, not just Copilot. However, it must be included here for completeness, especially since Copilot is deployed for efficiency rather than necessity in many cases.

9. The force must be able to demonstrate how they are complying with the Data Protection Act 2018 & GDPR:

Results are returned from Copilot to the user for them to review and accept or disregard. Copilot includes a warning for each prompt that generative AI products aren't guaranteed to be 100% factual.

Users must still use their judgement when reviewing the output before further processing. Copilot capabilities provide useful first drafts and summaries to help users achieve efficiency whilst still requiring human review. It is essential for the user to check the accuracy of outputs, particularly if any personal data is involved.

Users must not ask copilot to provide an answer which is beyond the users' knowledge and expertise, or which the user cannot otherwise ensure the output is correct.

Compliance with Force policy and data minimisation is supported through user manuals, data flows, Force Policy and regular briefings.

There are some specific areas of concern, namely that Microsoft has a central government contract to supply Copilot (and other services) across the UK public sector. This contractual arrangement does not allow for any specific regulatory requirements of any one sector and this includes compliance with Part 3 of the DPA18 for the processing of Law Enforcement Data as defined at ss29-31 DPA18. MS's own guidance is clear, 'it is not feasible for Microsoft to change its operational processes or create bespoke contractual commitments...for individual customers'.

In general terms, MS acts as a Data Processor when processing police data in Copilot Chat but it does retain the right to assume the role of Controller (that is a person who controls the purpose and means of processing) in respect of outputs produced through web-based searching. This is an important element of the need to keep web-grounding disabled. MS does not share data with 3rd parties without permission but does acknowledge that as a US-based company, it remains possible that they could be compelled to make disclosures under US domestic legislation and specifically the US CLOUD Act. As we do not have full control over MS as a Processor, there is an argument that the arrangement is not compliant with s59 DPA 2018.

Copilot may not have the ability to comply with the categorisation requirements at s39(3) DPA 2018.

Identifying and assessing risks

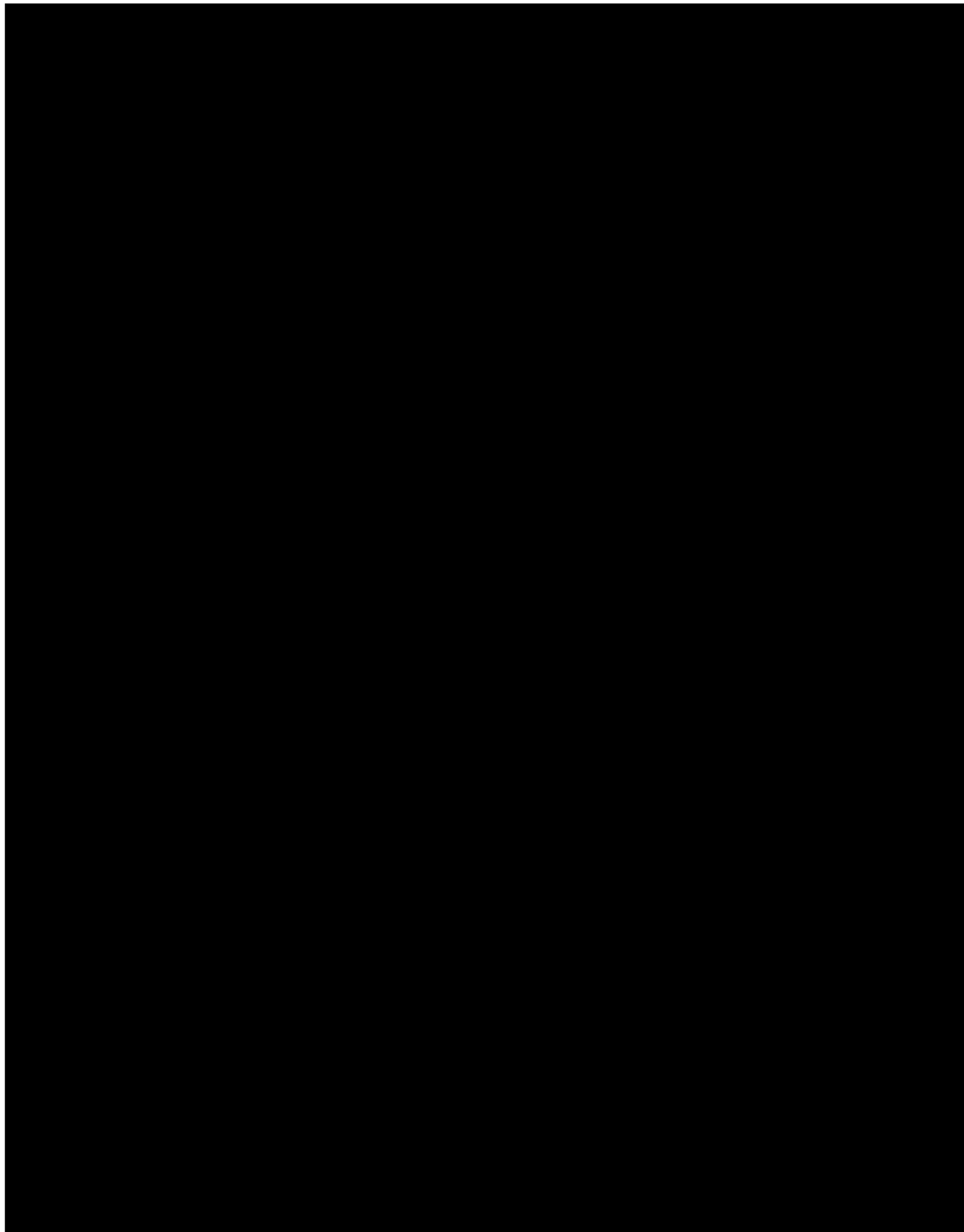
	Describe the risk, and <u>potential impact</u>	Likelihood	Severity	Risk	Agreed action	Action Owner	Risk score
1	<p>If data outside the approved AI decision flow is entered into a Copilot prompt, there is a risk that sensitive or unapproved data could be processed or stored, potentially resulting in a data breach involving personal or operational policing information.</p> <p>This would be a breach of processing under the Data Protection Act as opposed to a breach where data has left our network. Whilst this carries less risk (due to the mitigations detailed in the DPIA), this would still be recorded on the Force Breach Register and the member of staff / officer investigated.</p>	Possible	Significant	Medium	<ul style="list-style-type: none"> The Force has an established AI Governance Board that will liaise with Ethics Committees where necessary. The Force has implemented an AI Policy outlining acceptable and prohibited uses of AI tools. An AI Decision Flow document is available to guide users on appropriate queries and data entry. Web Grounding has been turned off which means Copilot will not send any data out to Bing. MS Purview is now being used which prevents Copilot from returning responses or using data in prompts that violate security policies, such as sharing sensitive data. Data on the Force network is no higher than Official-Sensitive classification. Data is encrypted in transit and at rest. Design follows PDS Blueprint 	Information Management / Information Security	Low
2	<p>There is a risk that Copilot could generate biased, inaccurate, or inappropriate content in responses. This could result in reputational damage, loss of public trust and potential legal or compliance issues. It could also lead to poor decisions making.</p>	Probable	Significant	Medium	<ul style="list-style-type: none"> Microsoft applies responsible AI principles and bias mitigation techniques. Human review of responses is recommended to ensure accuracy. Copilot is configured to respect user and organisational access controls. Web Grounding has been turned off which means Copilot will not send any data out to Bing. The Forces have undertaken staff training and produced policy, process maps and clear guidance that specifically state that outputs are the user's responsibility as is the necessity to conduct a detailed review of the accuracy. 	Information Management / Information Security	Low

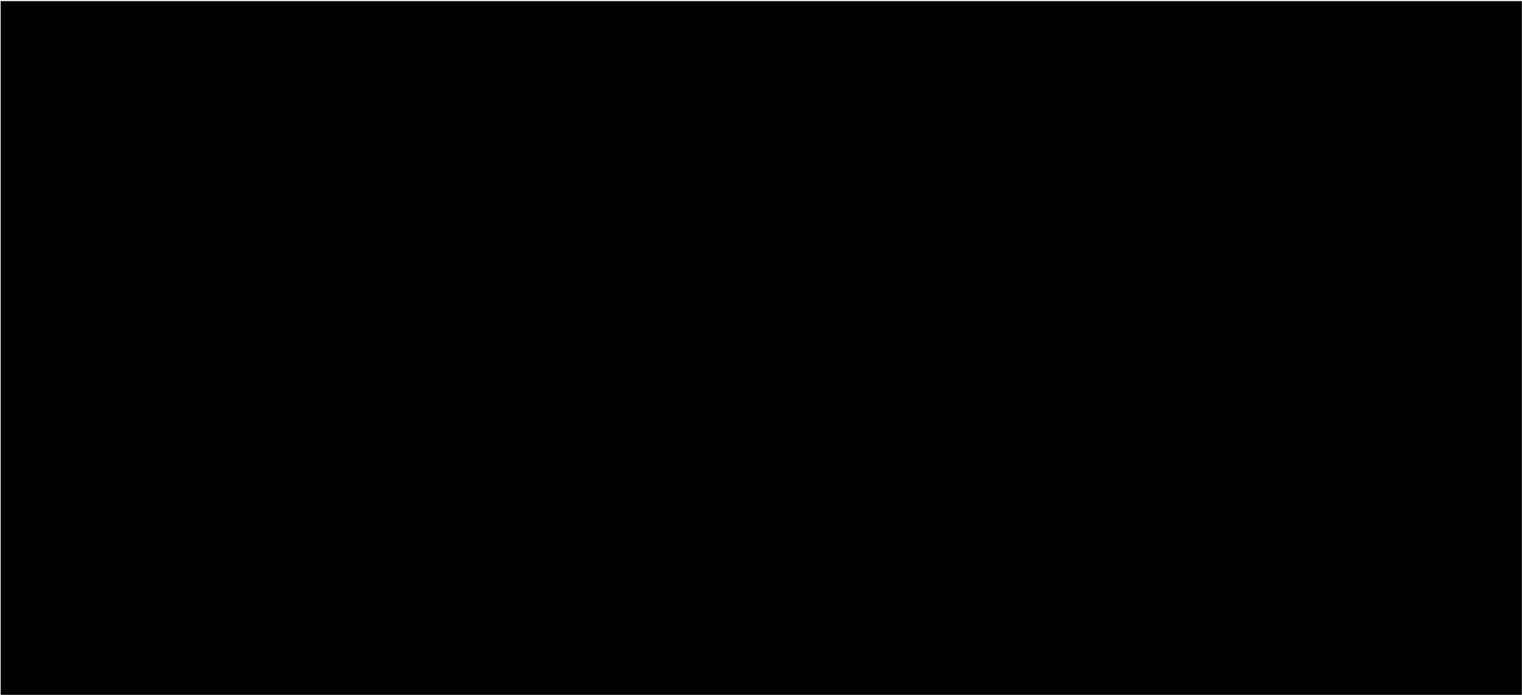
Authorisation of DPIA:

DPIA will be retained by the Information Governance team. This will be reviewed by the parties listed below with consideration then given for signatory by the Senior Information Risk Owner (SIRO), Senior Responsible Officer (SRO) and Information Commissioners Office (ICO) if required.

	Name	Date
Information Governance Officer		07/10/2026
Data Protection Officer Sussex		07/10/2026
Summary of DPO advice	<p><i>I have reviewed and offered comment on a previous iteration of this DPIA which will be retained for accountability and audit. The resulting amendments cover the high threshold for when processing of Sensitive or SC Data is 'strictly necessary', the need to take great care to review the accuracy of outputs in order to comply with the 4th Principle and clearly parameters regarding RRD.</i></p> <p><i>I have also asked that the risk assessment be updated to reflect that bias/inaccuracy is 'probable' rather than 'possible'.</i></p> <p><i>With these updates complete, I am satisfied that the risks from this processing are clearly set out and that the need for mitigation through clear and enforced SoPs is clearly understood.</i></p> <p><i>I have previously offered advice to chief officers regarding the risks associated with Copilot Chat in a report dated 13th Apr 26. All the concerns and recommendations set out in that report remain relevant. I do not propose duplicating in this DPIA but I will ask that the Apr 26 is attached as an Appendix.</i></p> <p><i>In summary, the overarching issues are:</i></p> <ul style="list-style-type: none"> <i>- The need to demonstrate necessity (as opposed to convenience)</i> <i>- Adherence to requirements regarding international transfers</i> <i>- The willingness/ ability of Microsoft to guarantee compliance with UK DP law.</i> <i>- Probabilistic responses and lack of transparency in conclusions.</i> <i>- The inability of the application to comply with the categorisation required at s38(3) DPA 18.</i> <i>- General concerns with RRD.</i> <p><i>I refer to the national DPIA prepared by the NPCC which states that 'it is likely that the majority of processing within Copilot Chat will not contain personal data'. The assessment also highlights that any Sensitive/ SCD processing or anything which presents a high risk to risk and freedoms will require a separate assessment beyond the 'general processing' DPIA. This local assessment is approved on the same basis.</i></p> <p><i>Sussex Police is ambitious in a desire to further exploit this technology and a number of new use cases are under consideration. I am satisfied that processing using pseudonymised data presents minimal risk and that purely corporate reports which include reference to named officers and staff (who as public servants have a lower expectation of privacy and are expected to be accountable) is also acceptable.</i></p> <p><i>The following are subject to ongoing review but will need mitigations build into SoPs before being approved:</i></p>	

	<ul style="list-style-type: none"> - Reports containing contractor/ supplier details - Summarisation of internal and external emails - Briefings and transcripts which include law enforcement data. 	
Data Protection Officer Surrey	██████████	09/10/2026
Summary of DPO advice	I can confirm Surrey Police are accepting of this DPIA and the risks associated with the use of Copilot within the force. I have no further comments or concerns that have already been raised, addressed or mitigated.	
Senior Information Risk Owner	██████████	12/10/2026
Summary	DPIA reviewed with the SIRO and amendments made to reflect. The document was approved on the 12/10/2026.	





Referral to the ICO (if required)

Refer Name	Date	ICO Comments

DPIA Review History

Date	IGO - Force	Comments