Data Protection Impact Assessment - NHS.net Connect (formerly NHSmail) M365 Copilot

Document filename:	**Data Protection Impact Assessment**	
Directorate / Programme	**Transformation Directorate**	
Document Reference *[insert IAR reference number]*		
Information Asset Owner	*John McGhie*	Version 2.0
Author	Jessica Davenport	Version issue date: 28 July 2025

Document Management

Revision History

Version	Date	Summary of Changes
1.0	October 2024	Pilot first draft
2.0	July 2025	Updates made for M365 Copilot General Availability

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
Paul Gardner	Information Governance Lead	October 2024	1.0
Hazel Randall	Associate Director of Legal	October 2024	1.0

Approved by

This document must be approved by the following people:

Name	Title / Responsibility	Date	Version
John McGhie	Head of Collaboration Services	July 2025	2.0

Document Control:

The controlled copy of this document is maintained in the NHS England corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

Purpose of this document

A Data Protection Impact Assessment (DPIA) is a useful tool to help NHS England demonstrate how we comply with data protection law.

DPIAs are also a legal requirement where the processing of personal data is *"likely to result in a high risk to the rights and freedoms of individuals"*. If you are unsure whether a DPIA is necessary, you should complete a DPIA screening questionnaire to assess whether the processing you are carrying out is regarded as high risk.

By completing a DPIA you can systematically analyse your processing to demonstrate how you will comply with data protection law and in doing so identify and minimise data protection risks.

This document should be read in conjunction with the DPIA Guidance and DPIA Screening Questionnaire.

1. Consultation with Stakeholders

The availability of M365 Copilot across NHS.net Connect includes the following stakeholders:

• NHS.net Connect programme leads - including service owners, SIRO, technical, solution assurance, information governance and security leads

• Accenture programme leads - including service owners, technical, information governance and security leads

• NHS England Privacy Transparency and Trust and Legal teams.

• NHSE organisation leads and participants

The NHS.net Connect Microsoft 365 Copilot pilot provided a consultation mechanism and obtained feedback from organisations on the feasibility of global roll out to the whole NHS.net Connect shared tenant. This consultation informed the prospect of making M365 Copilot globally available across the NHS.net Connect shared tenant and prompted the published Data Protection Impact Assessment to be updated.

2. Data Flow Diagram

Microsoft 365 Copilot is a generative Artificial Intelligence (AI) product, which automatically inherits the existing security, compliance, and privacy policies for Microsoft 365. In the current design, Microsoft 365 Copilot processes user-input ('prompts'), organisational data and content from the web to generate a response. User data is not used to 'retrain' the Copilot large language model. Results are returned from Copilot to the user, and it is then for the user to choose to use or disregard.

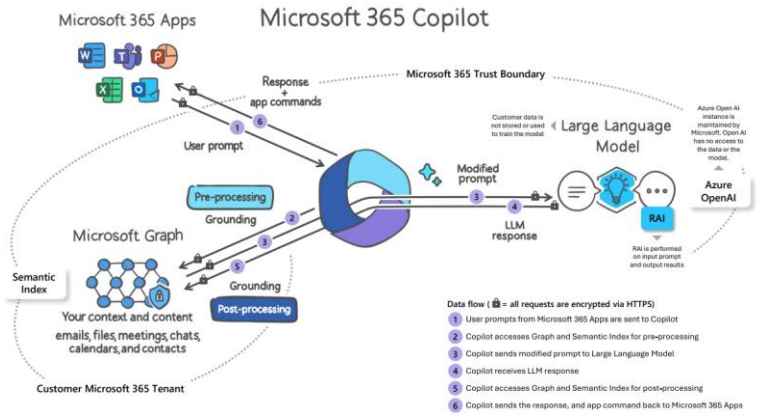
Microsoft 365 Copilot seamlessly integrates with the Microsoft 365 suite, including popular applications like Teams, Word, Outlook, PowerPoint, Excel, Loop and others. It aligns and depends on the M365 tenant configuration and setup to align with security, compliance, and privacy.

The communication between NHS.net Connect tenant and Copilot components is encrypted as a default.

As M365 Copilot operates within the NHS.net Connect tenant, patient information systems are out of scope e.g. but not limited to, the Person Demographics Service (PDS).

Plugins for M365 Copilot are extensions that enable Copilot to access and use third-party apps such as Bing Web Search. Copilot supports search-based message extensions (finding something in an external system and sharing the results with the conversation) as a plugin reviewed and approved by Microsoft in App Source. The web content plugin is enabled as default for all M365 Copilot users, which allows Copilot to reference web content to enhance responses to user prompts.

Below is a high-level diagram which depicts the information flows for Microsoft 365 Copilot. It begins when a user provides a 'prompt' (i.e. a command) within a Microsoft 365 app (e.g. Word). An example prompt could be 'generate a high-level project summary for MS Copilot'. This prompt is then processed using the user's content from within Microsoft 365 (e.g. your project meeting OneNote, a transcript from a weekly Copilot Teams meeting) via the Graph API, and provides an input to the Large Language Model which returns a response for further processing with the user's Microsoft 365 content before returning the response to the end user with the Microsoft 365 app (in this case the Project report within MS Word).



3. Purpose of the processing

This DPIA has been created to support local organisations with the completion of their local documentation and guidance for their local UK GDPR compliance.

Microsoft 365 Copilot is designed to assist with work-focused tasks within 365 apps like Word, Excel, and PowerPoint. Other instances of Copilot (e.g. Copilot Studio) are not within the remit of this DPIA (A comprehensive guide to Microsoft Copilot versions | ITWeb).

https://www.bing.com/ck/a?!&&p=81eae30dacbfe4faJmltdHM9MTcyNzc0MDgwMCZpZ3VpZD0wNGNiYmExOC04MmY0LTZlNjYtMTcyYS1hZWU5ODM4ZDZmMzkmaW5zaWQ9NTc5NA&ptn=3&ver=2&hsh=3&fclid=04cbba18-82f4-6e66-172a-aee9838d6f39&psq=microsoft+copilot+vs+365+copilot&u=a1aHR0cHM6Ly93d3cuZ2V0c3

VwcG9ydC5jby51ay9ibG9nLzIwMjMtMTEvbWljcm9zb2Z0LWNvcGlsb3QtdnMtbWljcm9zb2Z0LTM2NS1jb3BpbG90LXdoYXRzLXRoZS1kaWZmZXJlbmNlLw&ntb=1

The processing of information within the system is to support 'knowledge workers' to be more productive when using Microsoft 365 apps. An example of this would be automatically generating a project progress PowerPoint presentation based on a Microsoft Teams meeting attended, a project highlight report shared, and some project notes taken from Microsoft OneNote.

An Acceptable Use Policy for Microsoft 365 Copilot has been published on the NHS.net Connect Support Hub, local organisations are expected to share this with their users prior to granting a license (link to AUP).

4. Description of the Processing

Nature and scope of the processing:

NHS.net Connect is encrypted to a secure standard to allow document classifications of OFFICIAL (including the subset OFFICIAL SENSITIVE) to be stored and communicated, however NHS.net Connect should not be used as a replacement to any Patient Record System (but can be used in conjunction with, depending on local policies).

The existing data controller and processor arrangements are outlined in the published: NHS.net Connect Data Protection Impact Assessment - ENGLAND – Data Protection Impact Assessment – NHS.net Connect Support

And

ENGLAND – NHS.net Connect UK GDPR Joint Data Controller Table – NHS.net Connect Support

The general availability of M365 Copilot does not make any changes to existing UK GDPR roles and responsibility arrangements to NHS.net Connect organisations within the Microsoft tenant.

NHS England and each organisation implementing M365 Copilot are Joint Data Controllers for their respective roles:

- NHS England are the Data Controller for service configuration and provision
- Each organisation on the tenancy is Data Controller for the data they enter into NHS.net Connect
- Accenture is Data Processor acting upon instruction from NHS England and Microsoft are Sub-Data Processor

All records will be electronic.

M365 Copilot is not intended to be used in a way that produces any automated decisions regarding individuals. The data and documentation produced by Copilot results must be validated by users, as outlined in the M365 Copilot Acceptable Use Policy. This should be reinforced by local communications and training.

Description of processing:

Microsoft state: "Copilot presents only data that each individual can access using the same underlying controls for data access used in other Microsoft 365 services."

M365 Copilot can surface any information across the tenancy for which a user has at least 'view' permissions.

M365 Copilot documentation states it must not to be used for clinical decision-making, diagnostics, or as a substitute for a healthcare professional's expertise. The tool is not intended to support clinical care and cannot not be relied upon to inform treatment decisions, determine patient care pathways, or interpret clinical data.

As Microsoft 365 is not deployed as a clinical system across the NHS.net Connect tenancy we do not expect extensive patient data to be surfaced but this will depend how organisations and individuals currently utilise Microsoft 365 applications. It is up to an organisation's own discretion to decide what other use cases are acceptable and ensure DPIAs are created for these use cases. The same applies to any person identifiable data (e.g. HR records) stored within NHS.net Connect. Individual users will decide how to use any M365 Copilot outputs and are responsible for complying with local and national policies on their use of data and information.

Microsoft 365 Copilot is a Microsoft E5 licence add on and combines users' Microsoft 365 apps and data with a Large Language Model. The Copilot AI functionality is a productivity enhancement tool only to be used to help users with their existing work, assisting administrative tasks including writing, editing, summarising suggested content such as documents and presentations based on information and user prompts.

Microsoft set out the principles which they consider foundational to their commitment to customers:

- *"Built on Microsoft's comprehensive approach to security, compliance, and privacy. Copilot is built on top of and integrated with Microsoft 365. This integration enables you to take advantage of the existing Microsoft security, compliance, and privacy solutions that you've already deployed in your organization as well as other controls that may be made available to help you configure the use of Copilot as appropriate for your organization.*

- *Architected to protect tenant, group, and individual data. We know a major concern for customers is staying in control of access to business data within the organization. Within your tenant, we provide a permissions model that helps ensure that the right groups and users have access only to the data they're supposed to have access to.*

- *Committed to responsible AI. Microsoft is committed to making sure AI systems are developed responsibly and in ways that warrant people's trust. This work is guided by a core set of principles: fairness, reliability and safety, privacy and security, inclusiveness, transparency, and accountability*."

Further information on Microsoft 365 Copilot's privacy and security for can be found here: Data, Privacy, and Security for Microsoft 365 Copilot – Deploy Office | Microsoft Learn

Context of the processing (roles and responsibilities):

Organisations are responsible for training staff on appropriate use, storage and sharing of data.

Organisations are responsible for monitoring privacy settings for their organisations - O365 Privacy Monitoring – NHS.net Connect Support

The NHS.net Connect Joint Data Controller table outlines the separation of responsibilities for use of NHS.net Connect capabilities - ENGLAND – NHS.net Connect UK GDPR Joint Data Controller Table – NHS.net Connect Support

5. Describe the legal basis for the processing (collection, analysis or disclosure) of personal data?

Legal basis for collection and analysis: NHS.net Connect covered by direction issued by the Secretary of State for Health and Social Care where NHS England is appointed as the Service Provider for NHS.net Connect, taking responsibility for setting up and managing the data processing contract for the service on behalf of all Controllers.

Health and Social Care Act 2012 – Direction:

Informatics systems for the collection or analysis of information Directions 2016 - NHS England Digital

Local organisations are required to establish their own legal basis as outlined in the **ENGLAND – NHSmail UK GDPR Joint Data Controller Table – NHSmail Support.**

Legal basis for disclosure:

N/A

6. Demonstrate the fairness of the processing

Microsoft 365 Copilot will not be processing new data items; it will introduce a new way of surfacing data within the NHS.net Connect Shared Tenant to users with the relevant permissions.

ENGLAND – Transparency / Fair Processing Information – NHSmail Support

Transparency Note for Microsoft 365 Copilot | Microsoft Learn

7. What steps have you taken to ensure individuals are informed about the ways in which their personal data is being used?

Through guidance materials and the M365 Copilot Acceptable Use Policy, users are advised to use discretion when inputting data into Copilot (as 'prompts') as these inputs will directly affect the data processed by Copilot and the generated responses. Although Microsoft ensures that any data processed is secured, users can limit the personal data processed by Copilot by avoiding inputting sensitive details (including personally identifiable information) as prompts.

Acceptable Use Policy – NHSmail Support

8. Is it necessary to collect and process all data items?

Data items outlined in the published Data Protection Impact Assessment are processed subject to local organisation need and processes.

9. Describe if personal datasets are to be matched, combined or linked with other datasets? (internally or for external customers)

Microsoft Graph is a core component of M365 Copilot which binds M365 services and data together to synthesize and search content from multiple sources within an M365 tenant. Although M365 Copilot presents only data that each individual can access (using the same underlying controls for data access used in other Microsoft 365 services), the underlying model may combine or link personal datasets with other datasets to improve the quality of the response back to the user.

10. Describe if the personal data is to be shared with other organisations and the arrangements you have in place

N/A

11. How long will the personal data be retained?

M365 Copilot prompts and responses are retained for 180 days. This is part of the Teams retention policy.

Messages from Microsoft 365 Copilot and Microsoft Teams are automatically included in the retention policy location named **Teams chats and Copilot interactions** because they are retained and deleted by using the same mechanisms. Users don't have to be using Teams for the retention policy to apply to Copilot

Prompts and responses can be retrieved via forensic requests.

The forensic request for M365 Copilot will follow the existing Forensic Discovery request process - https://support.nhs.net/knowledge-base/forensic-discovery-requests/ by using the mailbox type as Copilot interactions are stored in a user mailbox.

12. Where you are collecting personal data from the individual, describe how you will ensure it is accurate and if necessary, kept up to date.

Personal Data - Personal data can be edited by the local organisations (Joint Controller) to ensure records are kept current.

NHS Directory and NHSmail Portal - This is maintained by the administrators in the local organisation employing the member of staff, it may be maintained either through the NHSmail Portal or through an automated synchronisation from a local directory (i.e., with TANSync). For certain fields (i.e., telephone number) the user can update these themselves through self-service.

Email, video conferencing and other collaboration data - Data quality for content sent over email or video conferencing capabilities or stored within other collaboration tools is the responsibility of the user sending / uploading the information. In the event it is incorrect the user should update and re-send / upload the corrected information.

13. How are individuals made aware of their rights and what processes do you have in place to manage such requests?

Organisations opt-in to M365 Copilot and must meet specified technical prerequisites.

Organisations must make users aware of the M365 Copilot Acceptable Use Policy prior to assigning a licence.

Users who received their M365 licenses as part of the pilot can withdraw from M365 Copilot by contacting their Local Administrator.

Data stored in NHS.net Connect regarding individuals may be processed by M365 Copilot, this will be outlined on the NHSmail support pages.

Useful links:

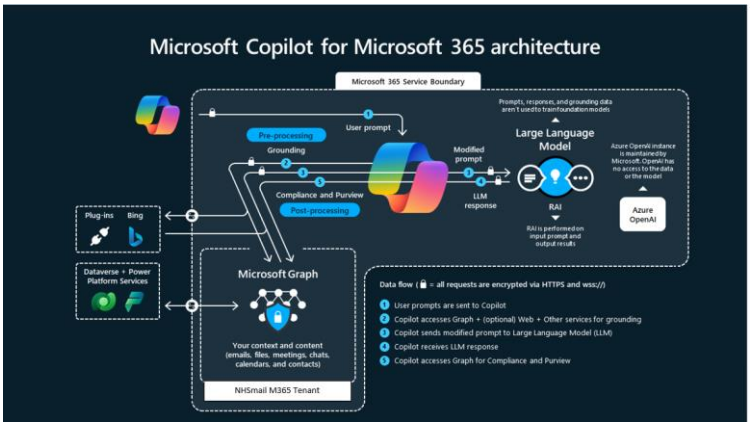
ENGLAND – Transparency / Fair Processing Information – NHSmail Support

Transparency Note for Microsoft 365 Copilot | Microsoft Learn

14. What technical and organisational controls for "information security" have been put in place?

Microsoft Controls

The communication between NHS.net Connect tenant and M365 Copilot components is encrypted as a default and the data architecture can be seen below. Data travels outside of the M365 Service Boundary to enhance Copilot responses with web content (Step 2).



Microsoft 365 Copilot automatically inherits the existing security, compliance, and privacy policies for Microsoft 365.

M365 Copilot uses search technology to ground a user's prompt in business data that is relevant to the prompt — i.e. consistent with the user's instructions. The more precise the prompt, the more likely M365 Copilot will use more precise grounding data for the prompt.

User data is not used to 'retrain' the Copilot large language model.

Enterprise Data Protection (EDP) for Copilot is turned on automatically on the tenant. EDP is a set of controls and commitments developed for consumers and protecting customer data while using the Copilot service. Some of the key aspects include:

- Data Security – Ensuring data is encrypted in transit and at rest.
- Privacy – Compliance with GDPR and ISO/IEC 27018 only to use data as instructed.
- Access Controls – Copilot can only access data it has been given access to – adhering to sensitivity labels, data retention policies and other administrative settings.
- AI Security – Protection against harmful AI-specific risks such as harmful content and prompt injections.
- Data isolation – Company data will remain isolated between tenants.

- No training on data – Data will not be used to train foundation models.

M365 Copilot's access to data

The nature of the NHS.net Connect shared tenant means that information configured to 'public' can be accessed by all NHS.net Connect users and potentially included in M365 Copilot results. This may be appropriate in some instances depending on the content.

The configuration of the existing 'Official Sensitive' labels, part of the Global Sensitivity Label Policy, will be updated to block M365 Copilot from accessing file content when any of these labels have been applied. The 'Official Sensitive' labels include three sub-labels: Recipients Have Full Control, Internal Use Editable & Internal Use Read Only. All three sub-labels will be updated to block M365 Copilot (via DLP Policy for Copilot).

Organisations will be automatically onboarded into the Global Sensitivity Labels policy during the M365 Copilot licensing onboarding process. Through guidance, organisations will be made aware of this pre-requisite and will be encouraged to opt-in to the Global Sensitivity Label Policy before submitting the request to onboard licenses.

M365 Copilot also respects Data Loss Prevention policies, which prevent the surfacing of sensitive information. Across the NHS.net Connect platform, there are two Data Loss Prevention (DLP) policies configured for SharePoint Online and OneDrive for Business:

1. **UK Data Protection Act** – This policy detects when a user attempts to share certain sensitive information.

Name	Description	Locations	Policy Settings	Conditions	Actions
UK Data Protection Act	To detect the presence of information subject to United Kingdom Data Protection Act and U.K. Personal Information Online Code of Practice (PIOCP) including data like: U.K. National Health Service Numbers U.K. Drivers Licence Number U.K. Electoral Roll Number U.S / U.K Passport Number SWIFT Code Credit Card Number EU Debit Card Number U.K. Unique taxpayer reference number Sensitivity Labels: Corporate / Recipients Have Full Control Official / Recipients	SharePoint sites, OneDrive accounts	UK Data Protection Act (Internal)	Content is shared from Microsoft 365 only with people inside my organization and contains sensitive info types	Notify users with email and policy tips
			UK Data Protection Act (External)	Content is shared from Microsoft 365 with people outside my organization and contains sensitive info types	Notify users with email and policy tips, restrict access to the content for external users
			Labelled Data (internal)	Content contains any of these sensitive info types: Official Data, Patient Identifiable Data and Personal Data Content contains any of these sensitivity labels: Corporate/Recipients Have Full Control, Corporate/Internal Use Editable, Corporate/Internal Use Read Only, Official/Recipients Have Full Control, Official/Internal Use Editable, Official/Internal Use Read Only, Official Sensitive/Recipients Have Full Control, Official Sensitive/Internal Use Editable, Official Sensitive/Internal Use Read Only	Notify users with email and policy tips

	Have Full Control Official Sensitive / Recipients Have Full Control Retention Label: Patient Identifiable and Personal Data Official Data		Labelled Data Content (External)	Content contains any of these sensitive info types: Official Data, Patient Identifiable Data and Personal Data Content contains any of these sensitivity labels: Corporate/Recipients Have Full Control, Official/Recipients Have Full Control, Official Sensitive/Recipients Have Full Control	Notify users with email and policy tips, restrict access to the content for external users

2. **Official and Public Data** – This policy is based on **the retention labelled applied** by users to their documents. These policies can automatically detect sensitive data across their data location. The configuration settings are described in the table below:

Name	Description	Location	Policy Settings	Conditions	Actions
Official and Public Data	Official and Public Data	SharePoint sites, OneDrive Accounts	Official and Public Data (Internal)	Content contains any of these sensitive info types: Official Data or Public Data. Evaluate predicate for Message or attachment	Notify users with email and policy tips
			Official and Public Data (External)	Content contains any of these sensitive info types: Official Data or Public Data. Evaluate predicate for Message or attachment	Notify users with email and policy tips

For further information go to Data Loss Prevention Guidance – NHS.net Connect Support

Additionally, a new Data Loss Prevention (DLP) policy specifically designed for Teams and Exchange Online has been created for M365 Copilot users, with the following settings:

Name	Description	Locations	Policy settings	Conditions	Actions
Copilot – Teams and Exchange Online DLP Policy	Policy for Exchange Online and Teams (Scoped to Copilot Licensing Group)	Exchange email - 1 account: NHS.net Connect | M365 Copilot Evaluation Programme. Teams chat and channel messages - 1 account: NHS.net Connect | M365 Copilot Evaluation Programme	U.K. Financial and Healthcare Data (External) - EXO and Teams	Content contains any of these sensitive info types: SWIFT Code, U.K. Driver's License Number, U.K. Electoral Roll Number, U.K. National Health Service Number, U.K. National Insurance Number (NINO), U.K. Unique Taxpayer Reference Number, U.S. / U.K. Passport Number, Credit Card Number, EU Debit Card Number Evaluate predicate for Message or attachment.	Notify users with email and policy tips. Restrict access to the content for external users

				And Content is shared from Microsoft 365 with people outside my organization	
			U.K. Financial and Healthcare Data (Internal) - EXO and Teams	Content contains any of these sensitive info types: Credit Card Number, SWIFT Code, U.K. Driver's License Number, U.K. Electoral Roll Number, U.K. National Health Service Number, U.K. National Insurance Number (NINO), U.K. Unique Taxpayer Reference Number, U.S. / U.K. Passport Number, EU Debit Card Number Evaluate predicate for Message or attachment. And Content is shared from Microsoft 365 only with people inside my organization.	

The DLP policy for Microsoft 365 Copilot helps prevent content labelled as 'Official Sensitive' from being included in Microsoft 365 Copilot responses during prompt summarization.

M365 Copilot Acceptable Use Policy (AUP)

M365 Copilot results are returned from Copilot to the user and are there for the user to choose to use or disregard. Copilot offers a warning once it has completed each prompt to outline to the user that the responses that generative AI produces aren't guaranteed to be 100% factual. Users should still review all outputs for inaccuracies, bias, confidential information or offensive content before sending them to others. Microsoft 365 Copilot capabilities provide useful drafts and summaries to help users achieve more while providing a chance to review the generated AI rather than fully automating these tasks.

It is essential for the user to check the accuracy of outputs, particularly if any personal data is involved. This forms part of the Acceptable Use Policy which all users should acknowledge prior to using M365 Copilot.

The AUP will serve as a standalone offline document available on the support site. Newly onboarded users to M365 Copilot (via BYOL) should be signposted to the AUP document on the support site. It will be the responsibility of each organisation to ensure their users are aware of the AUP. Additionally, signposting will be included within guidance to the orgs (through support site article).

15. In which country/territory will personal data be stored or processed?

Microsoft 365 Copilot data remains within the Microsoft cloud and content data is written in home region datacentres (in this case the UK).

The web content plug-in is enabled for all M365 Copilot users, allowing Copilot to reference web content to enhance responses to user prompts. When the web content plug in is enabled, Copilot generates a search query based on the user prompt (which could contain personal data) that is sent to the Bing Search API. This API uses the public Bing Search Infrastructure. This is not dedicated infrastructure, and the processing location cannot be controlled.

16. Does the National Data Opt Out apply to the processing?

No

17. Identify and assess risks

Consider the potential impact of your processing and the potential harm or damage that it might cause to individuals whether physical, emotional, moral, material or non-material e.g. inability to exercise rights; discrimination; loss of confidentiality; re-identification of pseudonymised data, etc.

You can also use this section to detail any risks you have in complying with data protection law and any resulting corporate risks e.g. impact of regulatory action; reputational damage; loss of public trust, etc.

Describe source of the risk and nature of potential impact on individuals.	**Likelihood of harm** (Remote; reasonable possibility or more likely than not)	**Severity of impact** (Minimal impact; some impact; or serious harm)	**Overall risk rating** (Low; medium; or high)
Risk 1: Risk of unauthorized access to data: Potential for M365 Copilot to highlight weaknesses in permissions across the NHS.net Connect tenant, in providing users with access to information that they should not be able to view.	Reasonable possibility	Some impact	Medium
Risk 2: Risk of data breaches: Unauthorised access may result in data breaches.	Reasonable possibility	Some impact	Medium

Risk 3: Risk of data misuse: Should a data breach occur, there is potential for users to misuse the output	Remote	Minimal impact	Low
Risk 4: Over permissive roles: Absence of robust mover and leaver process for permission management	Reasonable possibility	Some impact	Medium
Risk 5: Data residency: Data will be processed outside of the UK or EU geographical boundary for the purpose of web searches.	More likely than not	Some impact	Medium

17.1. Measures to mitigate (treat) risks

Against each risk you have identified, record the options/controls you have put in place to mitigate the risk and what impact this has had on the risk. Make an assessment as to the residual risk.

Also indicate who has approved the measure and confirm that responsibility and timescales for completion have been integrated back into the project plan.

Risk	Options to mitigate (treat) the risk	Effect on risk (Tolerate / Terminate / Treat / Transfer)	Residual risk (Low / Medium / High)	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
Risk 1: Risk of unauthorised access to data: Potential for M365 Copilot to highlight weaknesses in permissions across the NHS.net Connect tenant, in providing users with access to information that they should not be able to view.	Each M365 Copilot user is made aware of the M365 Copilot Acceptable Use Policy (AUP) prior to being provided a M365 Copilot licence. The M365 Copilot AUP outlines user responsibility, including escalation advice if M365 Copilot accesses data they should not have access to. User and administrator education drive to include NHS.net Connect shared tenant overview, information governance advice and M365 Copilot specific training. Local O365 Privacy Monitoring. Implementation of strict access controls and permissions management. Technical controls outlined in section 14. Ensuring that data processing adheres to specified purposes and	Treat	Low	John McGhie October 2024	

	implementing data minimization principles.				
Risk 2: Risk of data breaches: Unauthorised access may result in data breaches	Each M365 Copilot user is signposted to an Acceptable Use Policy (AUP) prior to being provided with an M365 Copilot licence. The AUP outlines user responsibility, including escalation advice if M365 Copilot accesses data they should not have access to. Local O365 Privacy Monitoring.	Treat	Low	John McGhie October 2024	
Risk 3: Risk of data misuse: Should a data breach occur, there is potential for users to misuse the output	User and administrator education drive to include NHS.net Connect shared tenant overview, information governance advice and M365 Copilot specific training. User's bound by own professional standards and obligation under the code of confidentiality.	Tolerate	Low	John McGhie October 2024	
Risk 4: Over permissive roles: Absence of robust mover and leaver process for permission management	As part of the migration to CoreView, the JML workflows have been updated so that when a user moves between an organisation outside of their existing parent-child ODS (which is deemed as the legal boundary) they get an entirely new account created. As part of the workflow the old account is renamed	Treat	Low		Pilot migrations are scheduled to start in the week commencing 25th August with mass migrations starting in the

	to allow the assigning of the UPN to the new account.				week commencing 29th September.
Risk 5: Data residency: Data will be processed outside of the UK or EU geographical boundary for the purpose of web searches.	Evaluate design decision to keep the web content plug-in (M365 Copilot) enabled.	TBC	TBC		

Commented [CL1]: Pending decision

18. Further Actions

- The completed DPIA should be submitted to the PTE Helpline Service for review
- The IAO should keep the DPIA under review and ensure that it is updated if there are any changes (to the nature of the processing and/or system changes)

19. Signatories

The DPIA accurately reflects the processing, and the residual risks have been approved by the Information Asset Owner:

Information Asset Owner (IAO) Signature and Date

John McGhie, July 2025