Data Protection Impact Assessment - NHS.net Connect (formerly NHSmail) Microsoft 365 Copilot Chat

Document filename:	**Data Protection Impact Assessment**	
Directorate / Programme		NHS.net Connect
Document Reference *[insert IAR reference number]*		Data Protection Impact Assessment - NHS.net Connect (formerly NHSmail) Microsoft 365 Copilot Chat
Information Asset Owner	*John McGhie*	Version 1.0
Author	NHS.net Connect team	Version issue date October 2025

Document Management

Revision History

Version	Date	Summary of Changes
0.1	21 July 2025	First review of draft

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
Jess Davenport	Service Manager	October 2025	0.1

Approved by

This document must be approved by the following people:

Name	Title / Responsibility	Date	Version
John McGhie	Head of Collaboration Services	October 2025	1.0

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 Microsoft 365 Copilot Chat was rolled out by Microsoft to all NHS.net Connect users as part of the functionality available within the Microsoft 365 licenses.

The following stakeholders were engaged for input / review of the DPIA:

- NHS.net Connect programme leads - including service owners, SIRO, technical, solution assurance, IG and security leads
- Accenture programme leads - including service owners, technical, IG and security leads
- NHS England Privacy Transparency and Trust and Legal teams

2. Data Flow Diagram

Microsoft 365 Copilot Chat (formerly Microsoft Copilot for Entra account users) is a generative AI service grounded in data from the public web in the Bing search index only and is available to all NHS.net users with the following licenses:

- Microsoft 365 E3
- Microsoft 365 F3
- Office 365 F3

This is a distinct offering from other available Microsoft Copilot products. For Microsoft 365 Copilot please refer to the Microsoft 365 Copilot pilot DPIA.

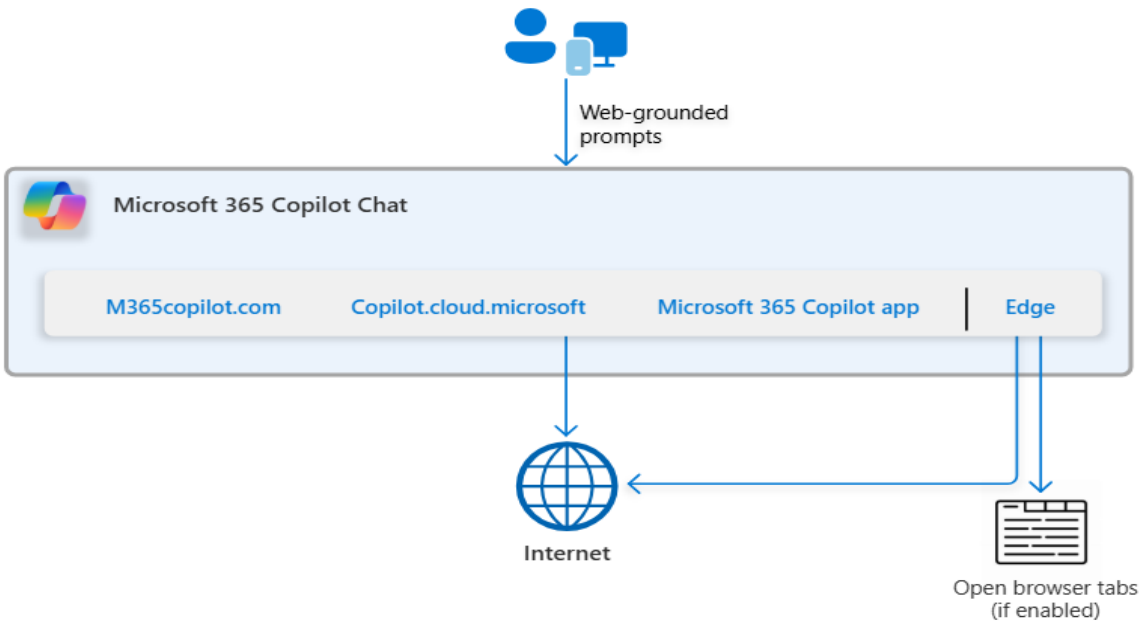
Unlike with Microsoft 365 Copilot (which requires an additional license), users cannot directly invoke organisational content like files, emails, or chats when interacting in Copilot Chat. Queries are run within the secure Nhs.net Connect tenancy but pulls information from the web.

Copilot Chat includes:

- Secure, AI chat grounded in the web and powered by GPT-5.0

- IT controls, including enterprise data protection and agent management
- Features such as Copilot Pages, file upload (for purposes of document summaries), and image generation

Below is a high-level diagram which depicts an information flow for Microsoft Copilot. It begins when users interact with Copilot Chat through M365copilot.com, Copilot.cloud.microsoft, the Microsoft 365 Copilot app, and Edge and generate a web-grounded prompt (i.e. a command). Copilot Chat only uses its internal pre-trained knowledge, and/or public currently available data to respond to prompts, unless browser page summarisation is enabled for Edge.



If
browser page summarisation is enabled for Edge by the organisation (managed locally by Intune or GPOs), the following web pages and document types can be summarised by Copilot in Edge:

- Intranet sites such as SharePoint, except embedded Office documents
- Outlook Web App
- PDFs, including those stored on the local device
- Sites not protected by Microsoft Purview DLP policies, Mobile Application Management (MAM) policies, or MDM policies

While Copilot Chat cannot invoke organisational content on its own, users can actively provide organisational content as part of their prompt for Copilot Chat to use in three ways:

1. Users explicitly type or paste this information directly into the chat
2. Users upload a file by selecting the "(+) Add content" button in the chat box. They can also drag and drop a file into the chat box. Uploaded files are stored in a user's OneDrive for Business as part of enterprise data protection within the NHS.net Connect tenant
3. Users type a prompt into Copilot Chat in Edge after enabling the 'Allow access to any webpage or PDF' setting, and an intranet page is open in the browser. In this scenario, Copilot may use this content to help answer questions

Additionally, users of the Microsoft 365 mobile app can click on suggested Copilot Chat prompts surfaced across the OneDrive, Capture, and Create tabs. In this scenario, the associated file and its content are used by Copilot Chat as part of the response. Users must adhere to local organisational policies relating to use of Mobile devices.

Copilot Chat does not use this uploaded data to train foundation models and Enterprise Data Protection (EDP) applies.

To help improve the quality of responses, Copilot Chat can use web search queries sent to the Bing search service to ground responses in the latest information from the web.

The Bing search service operates separately from Microsoft 365 and has different data-handling practices from those used for prompts and responses. These data-handling practices are covered by the Microsoft Services Agreement between each user and Microsoft, together with the Microsoft Privacy Statement. This means that Microsoft acts as an independent data controller responsible for complying with all applicable laws and controller obligations.

The following information is **not included** in the generated query sent to the Bing search service:

- The user's entire prompt, unless the prompt is very short (for example, "local weather")
- Entire files uploaded into Copilot Chat (uploaded files are stored in a user's OneDrive for Business as part of enterprise data protection)
- Entire web pages or PDFs summarised by Copilot Chat in Edge
- Any user or tenant identifiers (for example: username, domain, or tenant ID)

As part of providing the AI services, Microsoft will process and store inputs to the service as well as output from the service, for purposes of monitoring for and preventing abusive or harmful uses or outputs of the service.

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.

The NHS.net Connect shared tenant offers Microsoft Office licenses to all onboarded organisations, now including the Copilot Chat functionality.

The processing of information within Copilot Chat aims to support users with productivity and web-based queries. Users have the option as to whether to use the Copilot Chat functionality according to local organisation policies.

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

Use of Copilot Chat 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 that are part of the pilot 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. In relation to Bing search, Microsoft acts as an independent data controller responsible for complying with all applicable laws and controller obligations.

All records will be electronic.

Copilot Chat should not 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 Acceptable Use Policy. This should be reinforced by local communications and training.

Description of processing:

Copilot Chat is not grounded in enterprise data, therefore only the data which is directly uploaded to or referenced through Copilot Chat will be processed.

Users must be conscious of the personal, sensitive and clinical data they input into Copilot Chat and ensure they have appropriate permissions to process the data accordingly. Outputs will be subject to local organisational procedures.

Copilot Chat does not use uploaded data to train foundation models.

Context of the processing (roles and responsibilities):

Organisations will be responsible for ensuring suitable training and awareness on the use of AI tools and the appropriate use, storage and sharing of data.

Individuals using Copilot Chat will be responsible for adhering to local organisation policies and relevant Acceptable Use Policies (AUPs).

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

Copilot Chat is not grounded in enterprise data, therefore only the data which is directly uploaded to or referenced through Copilot Chat will be processed.

Users must be conscious of the personal, sensitive and clinical data they input into Copilot Chat and ensure they have appropriate permissions to process the data accordingly. Outputs will be subject to local organisational procedures.

Copilot Chat does not use uploaded data to train foundation models.

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

Only data which is included within prompts or uploaded to Copilot Chat will be processed. Users can decide as to the degree of their own personal data they wish to include. Users must follow local organisational policies when inputting personal, sensitive or clinical data relating to any other individuals, including ensuring that they have adequate permission to process the data.

Useful links:

ENGLAND – Transparency / Fair Processing Information – 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 and individual user needs.

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

N/A

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?

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

Messages from Microsoft Copilot Chat 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 do not have to be using Microsoft Teams for the retention policy to apply to Copilot.

Exchange mailboxes are used to store data copied from messages in Copilot. Data is stored in a hidden folder in the mailbox of the user. This hidden folder is not designed to be directly accessible to users or administrators but prompts and responses can be retrieved via forensic requests.

The forensic request for M365 Copilot Chat will follow the existing Forensic Discovery request process - https://support.nhs.net/knowledge-base/forensic-discovery-requests/ by using the mailbox type.

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

The accuracy of inputted/uploaded data will be the responsibility of the individual user. Responses generated by Copilot Chat cannot be considered entirely accurate/factual by default. It is essential for the user to check the accuracy of outputs, particularly if any personal data is involved, as outlined in the Acceptable Use Policy.

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

While the Copilot Chat functionality is enabled by default within the NHS.net Connect Microsoft Office licenses, the use of this functionality remains optional.

Users should be aware that other NHS.net Connect individuals may process any previously shared data (e.g. direct message, shared files, emails etc.) using Copilot Chat, including personal data.

Useful links:

ENGLAND – Transparency / Fair Processing Information – NHSmail Support

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

Technical and Organisational Controls:

- To use Microsoft 365 Copilot Chat, you must be signed in using your organisation NHS.net Connect credentials

- Identity and Access Management policies are in place, including the requirement for Multi-Factor Authentication (MFA)
- Data Classification & Data Sensitivity Policies
- Data Loss Prevention (DLP) capabilities
- 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.

Organisation / User-Specific Controls:

- Application of MFA
- Application of Data Sensitivity Labels

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

Residency:

Microsoft 365 Copilot Chat data residency commitments are outlined in the Microsoft Product Terms and Data Protection Addendum. In short, all prompts and responses are stored in the NHS.net Connect shared tenant in the UK (in a hidden folder in the user's mailbox) and are available for audit and eDiscovery.

Processing:

Microsoft 365 Copilot Chat requests are routed to the nearest regional data centres by default (UK, then EU). Web search queries sent from Copilot Chat to Bing are described in this document about how Microsoft handles generated search queries. In short, queries handled by Copilot are anonymised versions of the same queries that any user could submit by navigating to Bing.com. They also do not include all the prompt's content, but only a small subset of keywords selected to protect privacy. The exact query sent to Bing is disclosed to the user in the list of sources returned with the response.

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

N/A

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 Unauthorised Access: Potential for Copilot Chat to highlight weaknesses in permissions across the NHS.net Connect shared tenant, enabling users to upload data they should not have access to.	Reasonable possibility	Some impact	Medium
Risk 2: Risk of Data Misuse: Data used outside of the processing activities for which consent was provided.	Reasonable possibility	Minimal impact	Low

Risk 3: Use of Inaccurate Data: Lack of validation of accuracy of responses from Copilot Chat can lead to erroneous data being maintained.	Reasonable possibility	Minimal impact	Low
Risk 4: Risk of Data Breaches: Data exposure is possible if malicious actors have access to devices and use Copilot in Edge to produce summarisations of data from documents and sites.	Reasonable possibility	Some impact	Medium
Risk 5: Risk of Data Ingress/Merging: Data from within NHS.net Connect may be combined with data residing without NHS.net Connect as part of the Copilot Chat prompt and response.	Reasonable possibility	Minimal impact	Low

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)
Risk 1: Potential for Copilot Chat to highlight weaknesses in permissions across the NHS.net Connect shared tenant, enabling users to upload 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 and Copilot Chat specific training. Local O365 Privacy Monitoring Mitigated by implementing strict access controls and permissions management. Mitigated by technical controls outlined in section 14. Mitigated by ensuring data processing adheres to specified purposes and implementing data minimization principles	Treat	Low
Risk 2: Data used outside of the processing activities for which consent was provided	User and administrator education drive to include NHS.net Connect shared tenant overview, information governance advice and M365 Copilot and Copilot Chat specific training.	Tolerate	Low

	User's bound by own professional standards and obligation under the code of confidentiality		
Risk 3: Lack of validation of accuracy of responses from Copilot Chat can lead to erroneous data being maintained.	User and administrator education drive to include NHS.net Connect shared tenant overview, information governance advice and M365 Copilot and Copilot Chat specific training. User's bound by own professional standards to ensure that results are validated.	Treat	Low
Risk 4: Data exposure possible if malicious actor has access to device and uses Copilot in Edge to produce summarisations of documents and sites.	User and administrator education drive to include NHS.net Connect shared tenant overview, information governance advice and M365 Copilot and Copilot Chat specific training. Local O365 Privacy Monitoring Mitigated by implementing strict access controls and permissions management. Mitigated by technical controls outlined in section 14. Mitigated by ensuring data processing adheres to specified purposes and implementing data minimization principles	Treat	Low

Risk 5: Data from within NHS.net Connect may be combined with data residing without NHS.net Connect as part of the Copilot Chat prompt and response	User and administrator education drive to include NHS.net Connect shared tenant overview, information governance advice and M365 Copilot and Copilot Chat specific training. Local O365 Privacy Monitoring Mitigated by implementing strict access controls and permissions management. Mitigated by ensuring data processing adheres to specified purposes and implementing data minimisation principles. User's bound by own professional standards and obligation under the code of confidentiality.		

18. Further Actions

- The completed DPIA should be submitted to the PTE Helpline Service (ighelplineservice@nhsdigital.nhs.uk) 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 08 October 2025

20. Appendix A: References

Information included in this DPIA is based upon the following links is as per the available version as of 4 April 2025.

- https://learn.microsoft.com/en-us/copilot/overview#microsoft-365--chat-also-known-as--chat
- https://learn.microsoft.com/en-us/copilot/manage
- https://learn.microsoft.com/en-us/security/zero-trust/copilots/zero-trust-microsoft-copilot
- https://learn.microsoft.com/en-us/DeployEdge/edge-learnmore-copilot-page-summary-results
- https://learn.microsoft.com/en-us/copilot/privacy-and-protections
- https://learn.microsoft.com/en-us/copilot/microsoft-365/enterprise-data-protection
- Data, privacy, and security for web search in Microsoft 365 Copilot and Microsoft 365 Copilot Chat | Microsoft Learn
- https://learn.microsoft.com/en-us/purview/retention-policies-copilot
- https://support.microsoft.com/en-us/topic/copilot-in-bing-our-approach-to-responsible-ai-45b5eae8-7466-43e1-ae98-b48f8ff8fd44
- https://learn.microsoft.com/en-us/copilot/manage#microsoft-365--chat-eligibility
- https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-license-feature-overview
- Microsoft Services Agreement
- Microsoft Privacy Statement
- ENGLAND – Data Protection Impact Assessment – NHS.net Connect Support
- ENGLAND – NHS.net Connect UK GDPR Joint Data Controller Table – NHS.net Connect Support
- O365 Privacy Monitoring – NHS.net Connect Support
- ENGLAND – NHS.net Connect UK GDPR Joint Data Controller Table – NHS.net Connect Support
- ENGLAND – Transparency / Fair Processing Information – NHSmail Support
- EU Data Boundary
- Microsoft Product Terms and Data Protection Addendum
- How Microsoft handles generated search queries