Data Protection Impact Assessment – NHS.net Connect Copilot Extensibility

Document filename:	**Data Protection Impact Assessment**	
Directorate / Programme	**Transformation Directorate**	**NHS.net Connect**
Document Reference	**N/A**	
Information Asset Owner	*John McGhie*	Version 1.0
Author	CAN023 Project Team	Version issue date 26 Sep 2025

Document Management

Revision History

Version	Date	Summary of Changes
1.0	September 2025	Final version shared for publishing

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
Jessica Davenport	Service Manager	August 2025	1.0

Approved by

This document must be approved by the following people:

Name	Title / Responsibility	Date	Version
John Mcghie	Head of Collaboration Services	September 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 DPIA process for Copilot Extensibility involved engagement with key stakeholders across multiple domains to ensure comprehensive oversight and alignment with data protection standards.

- **Data Protection Officer (DPO):** Consulted to ensure compliance with GDPR and UK Data Protection Act requirements.
- **Information Security Team:** Provided guidance on security controls and risk mitigation measures for the AI platform.
- **NHS Digital/IT Operations:** Involved in reviewing infrastructure and integration with NHS.net environment.
- **Clinical Governance Leads:** Ensured the ethical use of patient and staff data within Copilot Extensibility.
- **User Representatives:** Early adopters and pilot users provided feedback on transparency, usability, and data privacy concerns.
- **Legal Counsel:** Reviewed the legal basis for processing and data sharing agreements with Microsoft.
- **CoPilot Studio Users:** Will be available to only a select number of individuals - this is managed by org LA and the corresponding security group associated with the Copilot Studio-enabled environment.

2. Data Flow Diagram

Copilot Studio full is a low-code development platform that will enable NHS organisationsto build, customise, and deploy AI-powered copilots tailored to their business needs. It provides a visual interface for designing conversational logic using topics, triggers, and generative AI, making it accessible to both technical and non-technical users. These copilots can connect to a wide range of data sources—including Microsoft Dataverse, SharePoint, and external APIs—allowing them to retrieve, process, and act on enterprise data in real time.

A key strength of Copilot Studio full lies in its governance and environment management capabilities:

- **Environments:** These provide isolated workspaces, helping teams manage lifecycle stages and maintain separation of concerns.
- **Data Loss Prevention (DLP) policies:** These enforce data governance by controlling how data can flow between connectors, such that sensitive information is not inadvertently exposed.
- **Role-based access control:** This enforces that only authorised users can modify or publish copilots, supporting secure collaboration across teams

Within the Power Platform ‘Environments’ are the building blocks of configuration and data storage. Copilots are built within an environment and are managed and controlled by that environment’s configuration. Environments only play a role for Copilot Studio Agents; they are not relevant to SharePoint Agents or M365 Agent Toolkit Agents. Within this section when we refer to environment, we will mean these configuration units.

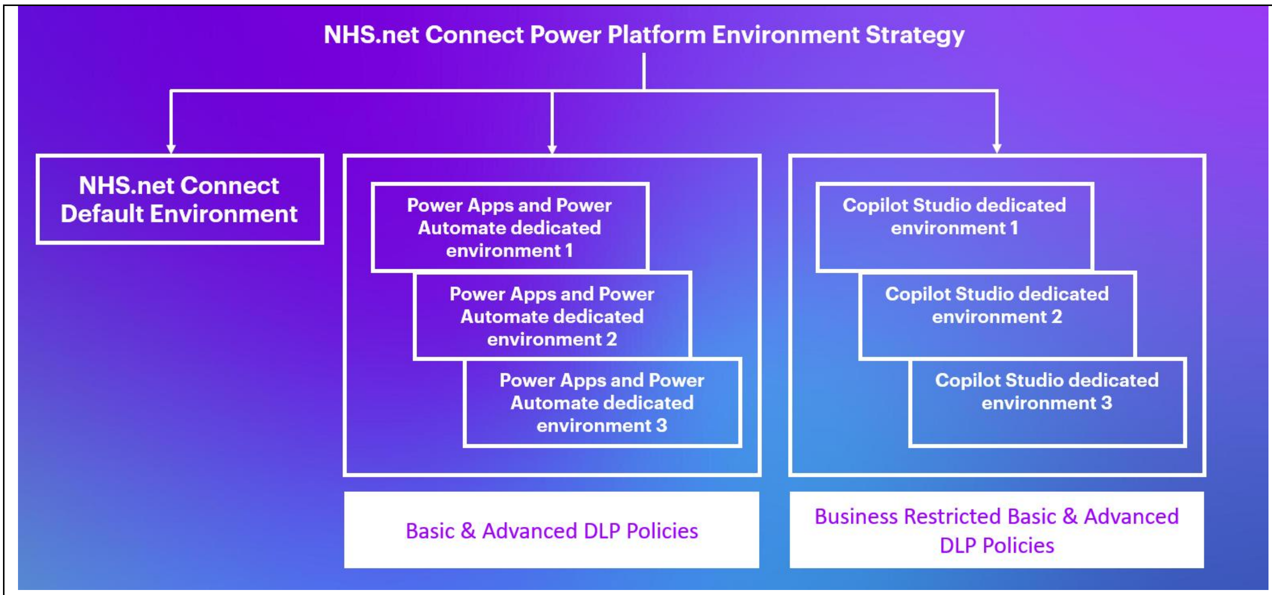
Organisations shall only interact with Copilot Studio full in nhs.net Production. Organisations shall not have access to the lower NHS.net Model Office (MO) and Development (Dev2) environments.

Environments are used today for building Power Platform solutions; the default environment is not used, a separate environment is created for each organisation.

Separate environments will be created for the use of Copilot Studio, forming a new category for the tenant as ‘Copilot Studio-enabled environments’. These will permit the use of Copilot Studio, whereas current environments will not. These environments will use separate DLP policies from the standard basic and advanced policies and will not use non-business data connectors.

This will result in two categories of environments:

- Power Apps and Power Automate only environments – Basic & Advanced DLPs
- Copilot Studio-enabled environments – Business Restricted Basic & Advanced DLPs



NHS.net Connect Power Platform Environment Strategy

NHS.net Connect Default Environment

Power Apps and Power Automate dedicated environment 1

Power Apps and Power Automate dedicated environment 2

Power Apps and Power Automate dedicated environment 3

Copilot Studio dedicated environment 1

Copilot Studio dedicated environment 2

Copilot Studio dedicated environment 3

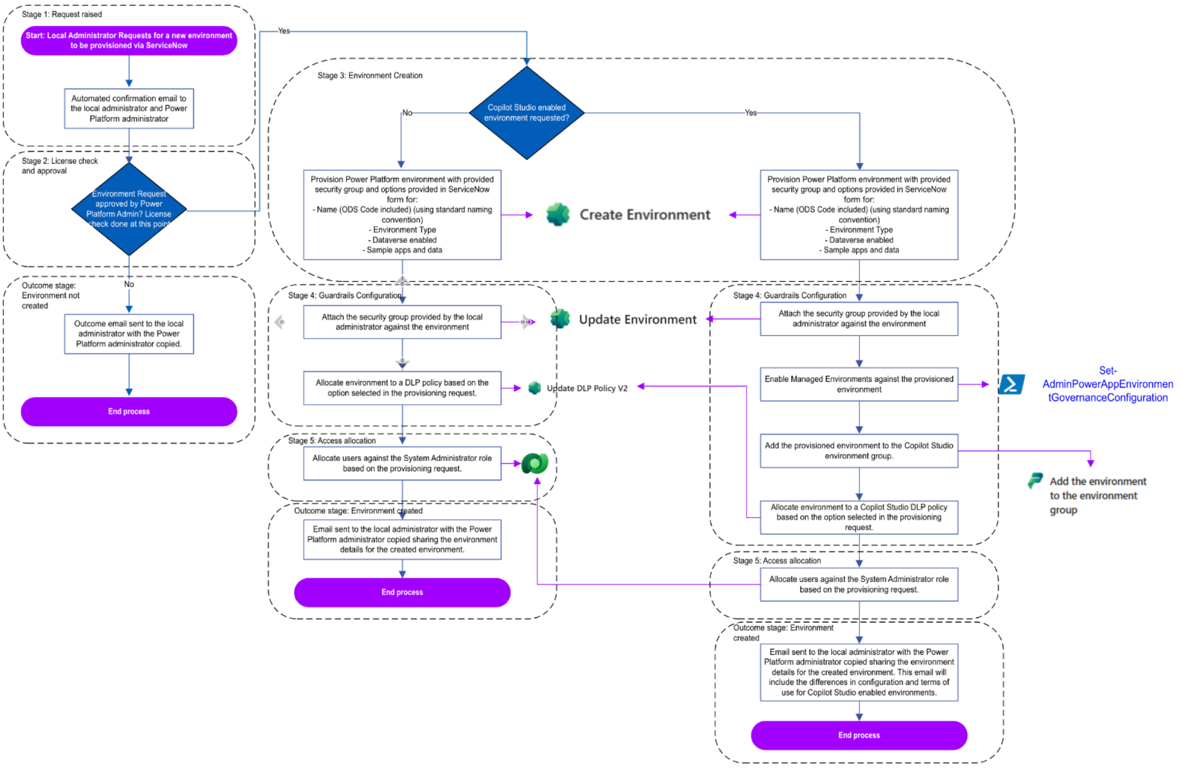
Basic & Advanced DLP Policies

Business Restricted Basic & Advanced DLP Policies

Based on local administrators' requests for an environment with Copilot Studio-enabled there are differences in provisioning an environment, from the normal process.

Currently to provision an environment the Power Platform Administrator uses a script or creates the environment based on the request details using the Power Platform Admin Centre (PPAC).

The diagram below highlights the process flow for environment request and provisioning.



Stage 1: Request raised

Start: Local Administrator Requests for a new environment to be provisioned via ServiceNow

Automated confirmation email to the local administrator and Power Platform administrator

Stage 2: License check and approval

Environment Request approved by Power Platform Admin? License check done at this point

Outcome stage: Environment not created

Outcome email sent to the local administrator with the Power Platform administrator copied.

End process

Stage 3: Environment Creation

Copilot Studio enabled environment requested?

Provision Power Platform environment with provided security group and options provided in ServiceNow form for:
- Name (ODS Code included) (using standard naming convention)
- Environment Type
- Dataverse enabled
- Sample apps and data

Create Environment

Stage 4: Guardrails Configuration

Attach the security group provided by the local administrator against the environment

Update Environment

Allocate environment to a DLP policy based on the option selected in the provisioning request.

Update DLP Policy V2

Enable Managed Environments against the provisioned environment

Set-AdminPowerAppEnvironmentGovernanceConfiguration

Add the provisioned environment to the Copilot Studio environment group.

Add the environment to the environment group

Allocate environment to a Copilot Studio DLP policy based on the option selected in the provisioning request.

Stage 5: Access allocation

Allocate users against the System Administrator role based on the provisioning request.

Outcome stage: Environment created

Email sent to the local administrator with the Power Platform administrator copied sharing the environment details for the created environment.

Email sent to the local administrator with the Power Platform administrator copied sharing the environment details for the created environment. This email will include the differences in configuration and terms of use for Copilot Studio enabled environments.

End process

Data Flow: Sources of Data for Copilot Studio Agents

The data accessed and processed by Copilot Studio agents will vary depending on the specific use case for which the agent is designed. Potential data sources include:

- **NHS.net Connect Systems:**
  Copilot agents may access data stored within NHS-managed systems and platforms where these have been added explicitly by the maker as knowledge sources for the agent. Access to such data is strictly controlled and governed under NHS data protection policies and only permitted when necessary for the agent's intended functionality.
- **User-Inputted Data:**
  End users (e.g., NHS staff) may input data directly during interactions with Copilot agents, such as queries, commands, or context information. This data is processed in real-time to generate responses and assist with tasks.
- **Public Data Sources:**
  Depending on the agent's design, it may also integrate publicly available data (e.g., medical guidelines, published research, or open government datasets) to enhance information quality. Use of public data adheres to licensing and usage terms and does not involve personal or sensitive data.
- **External Integrated Systems (if applicable):**
  In some use cases, Copilot agents might interface with third-party systems or APIs, where data exchange occurs under established data sharing agreements and strict security controls.

All data inflows and processing activities are subject to NHS governance frameworks, ensuring that only appropriate data is accessed, processed, or disclosed in accordance with user consent, legal bases, and data protection principles.

3. Purpose of the processing

The Copilot Studio service aims to safely introduce and evaluate AI-powered productivity and collaboration tools within a controlled NHS environment. The goal is to assess how Copilot Studio can enhance user efficiency, support clinical and administrative decision-making, and improve overall workflows while ensuring full compliance with NHS data protection, security, and governance standards.

Key objectives include:

- Validating the integration of Copilot Studio within the NHS.net Connect platform, including secure onboarding and user management.
- Assessing the effectiveness of data loss prevention (DLP) measures and managed environment controls to safeguard sensitive NHS data.
- Gathering user feedback to identify any risks, limitations, or operational issues related to AI-assisted interactions.
- Demonstrating that AI agents can be securely deployed without compromising patient confidentiality or data privacy.
- Informing future phases and broader rollout plans by establishing best practices for secure AI adoption in healthcare settings.

Copilot Studio is designed to enhance productivity and support clinical and administrative staff by providing AI-driven assistance within Microsoft 365 applications, including drafting, summarising, and data analysis features.

- To **improve user efficiency** by automating routine document creation and data processing.
- To support **clinical decision-making** by enabling rapid synthesis of information.
- To **streamline communication** and documentation workflows.
- To **enable secure collaboration** across NHS departments and teams.
- To leverage AI capabilities while maintaining stringent data protection and patient confidentiality standards.

The processing of information within Copilot Studio aims to support users with productivity and web-based queries. Users have the option as to whether to use the Copilot Studio 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 Studio does not make any changes to existing UK GDPR roles and responsibility arrangements to NHS.net Connect organisations.

NHS England and each organisation onboarded to NHS.net Connect 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 the Data Processor acting upon instruction from NHS England and Microsoft is the 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.

- **Data processed:** Personal data includes NHS staff information, clinical notes, patient identifiers (only where strictly necessary), emails, documents, and communication metadata accessed or generated within Copilot Studio.
- **Processing activities:** Ingestion of user-generated content (documents, emails), analysis by AI models to generate suggestions, summaries, or drafts, and temporary storage of data in encrypted Microsoft cloud environments.

Description of processing:

Copilot processing primarily uses the UK Azure OpenAI Service for prompt handling and generation. However, in certain scenarios, such as service fallback or capacity management the processing may occur in EU-based data centres. User prompts and responses are not solely stored in the user’s mailbox; depending on the specific Copilot workflow and integration points, additional storage locations within the Microsoft 365 ecosystem may be used.

Additionally, when Bing Search is invoked as part of Copilot functionality, associated data may be sent to and processed in the United States.

For more information on where different M365 services are hosted for NHS.net Connect visit - Data Retention and Information Management Policy – Office 365 – NHSmail Support.

Context of the processing (roles and responsibilities):

It is imperative for the NHS to determine the appropriate level of permissions required for LAs to execute monitoring and auditing responsibilities efficiently. A robust monitoring framework should include a combination of role-based access and visibility across platforms such as the Microsoft Admin Centre, Power Platform Admin Centre, and Viva Insights, depending on the desired granularity of oversight. The following structure outlines a proposed classification of roles and responsibilities within Copilot Studio, segmented into 3 key categories for clarity and operational alignment.

Environment Administrator – Accenture Support

This grants full access to the tenant and allows admin to manage, configure and monitor everything in the NHS tenant.

Microsoft Purview Audit Roles

These roles are intended for Security Admins who are responsible for safeguarding sensitive data, managing organisational risks, and ensuring adherence to regulatory requirements across cloud-based platforms. Admins with these permissions can audit user activity (e.g., who created, modified, or deleted agents)

Copilot Studio Roles

An Environment Maker or local administrator (LA) can delegate permissions to individuals or groups, allowing them to manage, edit, or view the agents they have created:

- Owner: Full control over the agent, including editing, publishing, and sharing
- Editor: Can modify and monitor the agent but cannot manage sharing settings.
- Viewer: Can only interact with the agent (e.g., chat), not monitor or edit it.

Lastly, organisations will be responsible for managing the acceptable use cases for Copilot Studio and ensuring that additional DPIAs are created where necessary for those use cases.

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

Health and Social Care Act (2012)

NHS England has a legal obligation (a Direction issued by the Secretary of State for Health and Social Care) that requires NHS England to establish and operate informatics systems and to exercise systems delivery functions including NHSmail as the national secure email service approved for sharing sensitive information. Health and Social Care Act (2012) – Section 254, Direction: “Novation of Information and Technology Contracts from DH to NHS Digital:

“Electronic Prescription Service, Health and Social Care Network, N3, NHS Choices, NHS e-Referral Service, Secondary Uses Service (SUS), Spine (Named Programmes) Directions 2016”

6. Demonstrate the fairness of the processing

Data processing by NHS England and Accenture to run and maintain the NHSmail Live Service

A document has been produced to confirm how the NHS.net Connect meets the UK GDPR duty of transparency and is called: NHS England (NHSmail Live Service) Transparency / Fair Processing Information. NHS.net Connect has a Copilot Agents specific Acceptable Use Policy (AUP) which staff (NHSmail users) are required to read and accept before the organisation is onboarded to the service. The AUP sets out the way the service runs, how users are expected to behave, and the data retention periods for data stored about them and the data that they send and receive via the NHSmail service.

Local organisations using NHS.net Connect are required to ensure their staff (NHS.net Connect users) have read and understood the policy documents and guidance provided. The Transparency / Fair Processing Information sets out how the NHS.net Connect complies with UK GDPR and should be used by NHSmail users in conjunction with the

Transparency / Fair Processing Information provided by their local organisations (as Joint Controllers). Local health and care organisations are responsible for briefing individuals referenced in this DPIA in relation to use of NHSmail and O365 tools.

Useful links:

ENGLAND – Transparency / Fair Processing Information – NHSmail Support

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 agents created by Copilot Studio 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.

No agents will be automatically grounded in broad tenant-level organisational data unless explicitly configured to do so.

Clear communication is provided via **NHS.net support materials** and user guides describing Copilot Studio's AI assistance functionality.

FAQs will be in place clarify the **purpose of building agents via Copilot Studio.** This will include common support queries with building agents and expected end user experience.

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)

There is **potential for datasets to be matched, combined, or linked**, depending on how individual agents are configured. Agent makers have the flexibility to design agents that reference **multiple knowledge sources**, which may include:

- Internal NHS.net Connect resources (e.g., SharePoint Online document libraries, Dataverse tables)
- Public or third-party data via approved external URLs

- User-provided inputs via the Copilot Studio interface

This configuration means that **data may be indexed and queried across multiple datasets**, resulting in dynamic responses that combine information from distinct sources for example, linking policy documents from a SharePoint site with reference information from a public-facing NHS webpage.

Considerations and Controls:

1. **Controlled Agent Configuration**
   a. Agent makers are responsible for defining which datasets an agent has access to. Access is scoped at environment level, and **Tenant Admins must review and approve** all agent deployments — ensuring alignment with data protection and governance requirements before publishing.
   b. Use of **external URLs** or APIs is reviewed as part of the agent approval workflow to prevent unauthorised or non-compliant data mixing.

2. **Disabled Connectors to Limit Risk**
   a) For the purposes of this service, high-risk connectors should be **explicitly disabled**, including. the **Direct Line Channel**, and **Copilot Studio (Autonomous Agents)**

3. **Manual Labelling and Dataset Sensitivity**
   a. Since sensitivity labels are applied manually in the NHS.net Connect tenant, there is a risk that datasets with different sensitivity levels (e.g., official vs. sensitive) may be queried together. Guidance has been issued to makers to apply appropriate labels and avoid combining data of inconsistent classification where not permitted.
4. **No External Sharing of Personal Data**
   a. Currently, there is **no planned sharing of personal datasets with external customers or organisations** as part of this service.
   b. All dataset usage remains internal to participating NHS organisations and is governed by existing NHS data protection policies and Microsoft tenant boundaries.

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?

Exchange mailboxes are used to store data copied from messages in Copilot. Data from generative AI messages is stored in a hidden folder in the mailbox of the user who runs the AI app. This hidden folder is not designed to be directly accessible to users or administrators, but instead, stores data that compliance administrators can search with eDiscovery tools.

The existing Retention policy for Copilot interactions is configured for 180 days of retention.

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 and agents created by Copilot Studio 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 Copilot Studio's functionality will be enabled for selected individuals within the NHS.net Connect Microsoft Office licences process.

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 Studio, 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 Studio, 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 is processed and stored within **Microsoft's Azure cloud**, compliant with NHS Digital's Data Security and Protection Toolkit (DSPT) standards.
- 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.
- Incident response and breach notification protocols are in place following NHS and GDPR regulations.

Organisation / User-Specific Controls:

- Application of MFA
- Application of Data Sensitivity Labels

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

Data is required to be processed in the UK/EU. To control and prevent data movement and processing in regions outside of the UK/EU, the terms of use controls within Power Platform environments can be unchecked (not accepted). This is by default a setting scoped at the environment level, which can be controlled at a tenant level using environment groups, a feature of Managed Environments.

Data Residency and Endpoint Validation

All agents must comply with NHS.net Connect data sovereignty requirements. This includes ensuring that any data processed or stored by the agent remains within the United Kingdom.

- API endpoints must process and store data within the UK.
- If UK-only processing is not possible, the endpoint must be explicitly reviewed and approved by the TDA.

- Agents must not use OpenAI, Azure OpenAI, or any other external LLM APIs.

For European Union (EU) users, Copilot Studio has additional safeguards to comply with the EU Data Boundary. EU traffic stays within the EU Data Boundary, while worldwide traffic can be sent to the EU and other countries or regions for LLM processing.

Microsoft 365 Copilot Studio data residency commitments are outlined in the Microsoft Product Terms and Data Protection Addendum.

Web search queries sent from Copilot Chat to Bing are not EUDB-compliant. Additional information is provided as to how Microsoft handles generated search queries.

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: Cross Organisation Data Oversharing: Oversharing and data leakage due to agents accessing or exposing data from other organisations. Agents can be configured to use author's credentials, which may lead to unauthorised access to sensitive resources.	More likely than not	Some impact	Medium
Risk 2: Lack of Full Monitoring of Copilot Agents via Sentinel: Lack of visibility of copilot agent granular activities such as admin activity, DLP violations and sensitivity label events	More likely than not	Some impact	Medium

Risk 3: Bing Search Service for Copilot Agent (Data Processing): Processing of enterprise data and user prompts based outside the UK or EU, which has regulatory implications	More likely than not	Some impact	Medium
Risk 4: Autonomous Agents Exploitation: Autonomous agents can increase the risk of data exfiltration if compromised or badly-designed. Unauthorised decision making by autonomous agents could lead to malicious activities	More likely than not	Serious harm	High
Risk 5: API Plugins in Microsoft 365 Agents Toolkit could lead to data exfiltration: Risk of data exfiltration where agents can be used with both enterprise data and any API that a maker chooses.	More likely than not	Serious harm	High
Risk 6: Pre-existing Environments for Copilot Agent: Copilot Studio agents may have been created in pre-existing Power Platform environments that lack appropriate controls (e.g. RBAC, DLP, audit logging, content moderation). This creates a live risk of data exposure, misuse, or inappropriate model outputs.	Reasonable Possibility	Some Impact	Medium
Risk 7: Middleware API Data Exfiltration: New untested MCP servers can be of value to makers of agents, although there can be unknown risks and security issues when servers have not been adequately tested	Reasonable Possibility	Some Impact	Medium

Risk 8: Microsoft Copilot Studio Lite: Risk of sensitive data being stored without being encrypted by the Customer Managed Key (CMK):	Reasonable Possibility	Some Impact	Medium
Risk 9: Risk of Unauthorized Access: Potential for Copilot Studio to highlight weaknesses in permissions across the NHS.net Connect tenant, enabling users to upload data they should not have access to	Reasonable Possibility	Minimal Impact	Low
Risk 10: Risk of Data Misuse: Data is used outside of the processing activities for which consent was provided.	Reasonable Possibility	Minimal Impact	Low

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	**Current mitigations to (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: Cross Organisation Data Oversharing	• NHS will only share agents that enforce user credentials use and discourage the use of author credential for building agents in Copilot Studio. • Copilot Studio Agents created would require TDA and security approval before publishing, so agents are only shared to appropriate organisations and users will be auto-approved, while Agents created in Agents Toolkit using external APIs would require TDA and security approval before publishing.	Treat	Medium	John McGhie, September 2025	
Risk 2: Lack of Full Monitoring of Copilot Agents via Sentinel	• M365 Audit logs are connected to Sentinel; therefore, copilot interactions are captured.	Treat	Medium	John McGhie, September 2025	

	• Define Monitoring Use Cases / Continuous Monitoring Uplift				
Risk 3: Bing Search Service for Copilot Agent (Data Processing)	• Continue work with Microsoft on how M365 Copilot uses Bing search for web grounding • Conduct a Privacy Impact Assessment (PIA) for Copilot agent usage, including Bing integration to better understand the risks,	Treat	Medium	John McGhie, September 2025	
Risk 4: Autonomous Agents Exploitation	• Microsoft Copilot Studio (connector) will be blocked to prevent use of autonomous agents (triggers) • Any requests for Autonomous Agents should be raised as an exception and approved via the TDA process	Treat	Low	John McGhie, September 2025	
Risk 5: API Plugins in Microsoft 365 Agents Toolkit could lead to data exfiltration	• Side-loading is disabled which prevents use without submission for review through • Only allowed agents are declarative (JSON key and value combinations, not custom code) and scripted	Treat	Low	John McGhie, September 2025	

	checks will be performed as first check. • Highlight in Terms of Reference (ToR) for Pilot and Organisational Acceptable Use Policy (AUP) for GA				
Risk 6: Pre-existing Environments for Copilot Agent	• Controls have been implemented for GA environments, although this risk is currently live and cannot be mitigated until adequate controls are implemented for risks raised	Treat	Low	John McGhie, September 2025	
Risk 7: Middleware API Data Exfiltration	• Copilot Studio-enabled environment – Business restricted Basic and Advanced Data Loss Protection (DLP) policies will be enabled • External API connectors will be blocked for use with Copilot Agents. • It's Recommended that NHS conducts ongoing security assessment of custom endpoints hosted by the organization, by the relevant security team aligned to the organization • Highlight in Terms of Reference (ToR) for Pilot and	Terminate	Low	John McGhie, September 2025	

	Organisational Acceptable Use Policy (AUP) for GA				
Risk 8: Microsoft (Copilot Studio) Agent builder	• Highlighted in ToR for Pilot and Organisational Acceptable Use Policy (AUP) for GA • Highlight risk to NHS England if Customer Managed Key (CMK) is used for other services (TBC), otherwise take no action.	Terminate	Low	John McGhie, September 2025	
Risk 9: Risk of Unauthorised Access	• User and administrator education drive to include NHS.net Connect shared tenant overview, information governance advice and Copilot Studio specific training. • Mitigated by implementing strict access controls and permissions management. This is managed by organisation LA and the corresponding security group associated with the Copilot Studio-enabled environment • Mitigated by ensuring data processing adheres to	Treat	Low	John McGhie, September 2025	

	specified purposes and implementing data minimization principles				
Risk 10: Risk of Data Misuse	• User and administrator education drive to include NHS.net Connect shared tenant overview, information governance advice and Copilot studio specific training. • User's bound by own professional standards and obligation under the code of confidentiality	Tolerate	Low	John McGhie, September 2025	

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, September 2025