NHS
Counter Fraud Authority

Microsoft Teams

Data Protection Impact Assessment

August 2021

V3.0 Published

NHS fraud.
Spot it. Report it.
Together we stop it.

Executive Summary

This document contains information in relation to the Microsoft Teams

Microsoft Teams is a unified communications and collaboration platform with document sharing, online meetings and many more useful features for business communications. It is part of the Microsoft 365 suite of applications designed to simplify group work

Teams is an office productivity tool used mainly for communication between people and exchanging messages in a channel as part of a project or group activity. Teams has 3 main features

Chat – Chat with anyone in the organisation and all the conversations are searchable.

Conferencing – Conduct online meetings and video calls which includes screen sharing.

Collaboration – Integrates with different business applications from third party providers.

This document is deemed OFFICIAL and any information viewed/obtained within this document should be treated in the appropriate manner as advised and set out in the Government Security Classifications (May 2018).

More information in relation to this data classification, including the requirements for working with these assets can be found here:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

In particular please note that:

ALL routine public sector business, operations and services should be treated as OFFICIAL - many departments and agencies will operate exclusively at this level. There is no requirement to explicitly mark routine OFFICIAL information. Baseline security measures should be enforced through local business processes. A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL–SENSITIVE'**

Table of contents

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Security and Operational Support Specialist	DPIA / Microsoft Teams	DPO	V0.1	August 2020	Initial creation
Security and Operational Support Specialist	DPIA / Microsoft Teams	DPO	V0.2	September 2020	Updates
Security and Operational Support Specialist	DPIA / Microsoft Teams	DPO	V0.3	September 2020	Final updates
Security and Operational Support Specialist	DPIA / Microsoft Teams	DPO	V1.0	September 2020	Final
Security and Operational Support Specialist	DPIA / Microsoft Teams	DPO	V2.0	August 2021	Redacted for publication
Security and Operational Support Specialist	DPIA / Microsoft Teams	DPO	V3.0	February 2023	Redacted further Original completion date retained as no change to process

Prefix	
Reference:	**DPIA Microsoft Teams**
Date:	**August 2021**
Author:	**Security and Operational Support Specialist**
Data Owner:	**NHSCFA**
Version:	**3.0**
Supersedes	**2.0**

Links & Dependencies

Document	Title	Reference	Date	POC
DPA	Data Protection Act	All	2018	HMG
EU GDPR	EU General Data Protection Regulation	All	2016	GDPR
FOI	Freedom of Information Act	All	2000	HMG
Government Security Classifications	Government Security Classifications	All	May 2018	Cabinet Office
HRA	Human Rights Act	All	1998	HMG
ISO/IEC 27000	Information security management systems Standards	ISO/IEC 27001:2013	Oct 2010	ISO
IS1P1 & P2	HM Government Infosec Standard No. 1, Part 1 – Risk Assessment and Treatment	P1 - Issue 3.5 P2 – Issue 3.5	October 2009 October 2009	CESG
IS2	InfoSec Standard 2	Issue 3.2	January 2010	CESG
PECR	The Privacy and Electronic Communications Regulations	All	2003	HMG

1. Data Protection Impact Assessment Requirement & Process

Introduction

1. The General Data Protection Regulation (GDPR) 2016 introduces a new obligation to undertake Data Protection Impact Assessments (DPIAs), before carrying out types of processing **'likely to result in high risk(s) to individuals' interests'**. DPIAs are now mandatory for certain types of processing and there are specific legal requirements for content and process. Where a DPIA identifies a 'high risk' that cannot be mitigated, the Information Commissioner's Office (ICO) must be consulted.
2. DPIAs provide a way to systematically and comprehensively analyse the intended processing and help to identify and minimise data protection risks. In addition to considering compliance risks, they should also consider broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm to individuals or to society at large, whether it is physical, material or non-material.

3. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It does not have to eradicate the risks altogether, but should help to minimise them and assess whether or not remaining risks are justified. A DPIA may cover a single processing operation or a group of similar processing operations. For new technologies you may be able to use a DPIA done by the product developer to inform your own DPIA on your implementation plans.

4. A DPIA must consider 'risks to the rights and freedoms of natural persons'. While this includes risks to privacy and data protection rights, it can also affect other fundamental rights and interests:

   "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead **to physical, material or non-material damage**, in particular: where the processing **may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy**, **unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage**; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data[1]…"

5. Under GDPR you must carry out a DPIA where for example you plan to:

   a. process special category or criminal offence data on a large scale.

6. The ICO also requires a DPIA to be undertaken for example, where you plan to:

   a. use new technologies;

   b. match data or combine datasets from different sources;

   c. collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');

7. DPIAs are an essential part of the organisation's accountability obligations under GDPR and an integral part of the 'data protection by default and design approach'. An effective DPIA helps to identify and fix problems at an early stage, demonstrate compliance with data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur.
8. Conducting a DPIA is a legal requirement for any type of processing. Failure to carry out a DPIA in required cases may leave the organisation open to enforcement action, including a **fine of up to €10 million**.

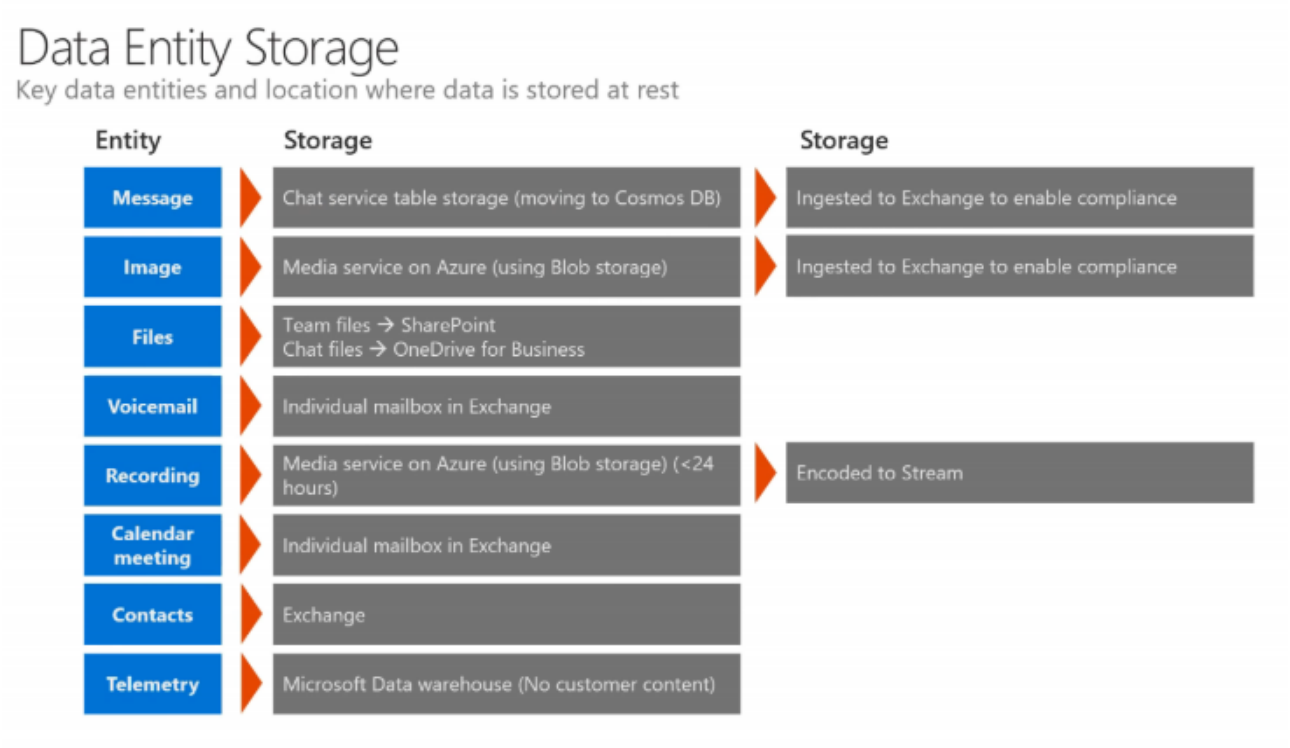
[1] GDPR - Recital 75

9. This DPIA is related to the NHSCFA Risk Assessments, which outline the threats and risks. The Risk Assessment document was developed in accordance with the requirements of NHSCFA and CESG HMG Infosec Standards 1 and 2.

Microsoft Teams General Description

10. Microsoft Teams is chat based collaboration platform complete with document sharing, online meetings and many useful features for business communication. Having a team space is a key to make creative decisions and communicate with members who might be spread across the globe.

11. Microsoft Teams stores different kinds of data in different kinds of services or applications. The Data Entity Storage model below shows where Microsoft Teams stores its different data.



12. As indicated above, there are features available in Teams. These will be subject to a separate DPIA. They include as highlighted:
    a) meetings recorded in Teams stored in **Microsoft Stream**
    b) files stored in **Sharepoint and OneDrive**
    c) chats stored in **Microsoft Exchange**

13. The database is accessed by all members of staff from NHSCFA, and for security and confidentiality purposes there are only 3 teams service system administrators. These administrators can only configure teams and cannot access any data.

14. This is the only DPIA to be completed on Microsoft Teams and it has been carried out by the Information and Records Management Officer, in consultation with the Security & Operational Support Specialist and the Information Governance and Risk Management Lead.

15. The platform, in addition to GDPR is also required to comply with other relevant HMG legislation including where applicable the Data Protection Act 2018, Human Rights Act 1998 and Freedom of Information Act 2000.

Data Protection Impact Assessment

16. To ensure the platform meets all legal requirements and the risks to personal data are identified and understood it is necessary to undertake a DPIA. This DPIA is based on the ICO's recommended template[2] comprised of seven steps:
    a. Step 1 - Identify the need for a DPIA
    b. Step 2 - Describe the processing
    c. Step 3 - Consultation process
    d. Step 4 - Assess necessity and proportionality
    e. Step 5 - Identify and assess risks
    f. Step 6 - Identify measures to reduce risk
    g. Step 7 - Sign off and record outcomes

[2] Version 0.3 (20180209)

STEP 1: Identify the need for a DPIA

Explain broadly what the system/project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Microsoft Teams as mentioned above is a collaboration tool. Teams is deeply integrated with Office365 suite of applications. Some of the features of teams are

- Chat and instant messaging
- Manage calendars and meetings (Outlook)
- Create, share, edit and find content (SharePoint, OneDrive)
- Call and meet team members
- Integrate with to-do lists (Planner)
- Integrate with 3rd party Apps through Tabs, Connectors and Bots

Microsoft processes data as part of the service offering. The data includes

- **Content:** Meetings and conversations chats, voicemail, shared files, recordings and transcriptions. However, staff were made aware in the Teams guidance, that the content should not include special category or criminal convictions data. This will be reiterated and made explicitly clear via regular updates through publication channels such as the staff intranet Go2.
- **Profile Data:** Data that is shared within your company about you. Examples include your E-mail address, profile picture, and phone number.
- **Call History:** A detailed history of the phone calls you make, which allows you to go back and review your own call records.
- **Call Quality data:** Details of meetings and call data are available to your system administrators. This allows your administrators to diagnose issues related to poor call quality and service usage.
- **Support/Feedback data:** Information related to troubleshooting tickets or feedback submission to Microsoft.
- **Diagnostic and service data:** Diagnostic data related to service usage. This personal data allows Microsoft to deliver the service (troubleshoot, secure and update the product and monitor performance) as well as perform some internal business operations, such as:

STEP 2: Describe the processing

Describe the nature of the processing:

1. How will you collect, use, store and delete data?

2. What is the source of the data?

3. Will you be sharing data with anyone (consider using a flow diagram or other way of describing data flow)?

4. Why types of processing identified as 'likely high risk' are involved?

1.Data is collected, used and stored as per Organisation acceptable use policy, and to also fulfil the organisation's public task function. Chats and conversations in channels have retention period of 180 days and then they are deleted. This does not apply to recordings.

2.Source of the data is communications among staff used for official business purposes, and although personal communication is permitted this should be limited. There is also communication with stakeholders, however this isn't automatic as it is up to the individual team owner to add external people as guests.

3.Data is not shared with anyone and the data residing on the cloud is only accessible to the customer as per Microsoft guidelines.

4.There is a risk of accidental sharing of files with outside vendors and partners
e.g. As a result of a successful compromise of the Microsoft network by an attacker originating from the internet, there is a risk that they could gain access to servers hosting the Teams servers or components of the Teams servers, which may result in a loss of data/denial of services. However as stated previously, we are not permitting the sharing of official sensitive documents.

Describe the scope of the processing:

1. What is the nature of the data and does it include special category or criminal offence data?

2. How much data will you be collecting and using?

3. How often?

Data is collected on a continuous basis which applies to all the NHSCFA Staff.

4. How long will you keep it?

5. How many individuals are affected?

6. What geographical area does it cover?

1. The nature of the data involves organisational business communications and documents. It does not include official sensitive, special category or criminal offence data, which was stipulated in the initial guidance released when Teams was introduced

2. Data is collected on a continuous basis which applies to all the NHSCFA Staff.

3. Data is collected on a continuous basis.

4. Data retention policy for chats and conversations is 180 days which applies to all NHSCFA Staff. It does not apply to recordings.

5. This applies to all the NHSCFA Staff

6. England and Wales

Describe the context of the processing:
1. What is the nature of your relationship with the individuals? 2. How much control will they have? 3. Would they expect you to use their data in this way 4. Do they include children or other vulnerable groups? 5. Are there any prior concerns over this type of processing or security flaws? 6. Is it novel in any way? 7. What is the current state to technology in this area? 8. Are they any current issues of public concern that you should factor in? 9. Are you signed up to any approved code of conduct or certification scheme (once any are approved)?
1. The relationship is mainly with NHSCFA Staff, however there may also be relationships with external third parties when they are invited to join a conversation by the owner of a team. 2. Staff can only chat, join a team and share files as part of collaboration activity. 3. All NHSCFA Staff when onboarding have to agree to the Acceptable Use Policy 4. No 5. No 6. No, the platform is well established in business. 7. Many organisations are using this platform for business collaboration. 8. No 9. The NHSCFA has an ISO ISO27001:2013 certification on information security which covers information processed within the NHSCFA network. The certification held for Teams is explained in Step 4 below.

Describe the purposes of the processing:

1. What do you intend to achieve?

2. What is the intended effect on individuals?

3. What are the benefits of the processing, for you and more broadly?

1. Enable improved communication and collaboration for the organisation?

2. Enable staff to have more opportunity of internal and external engagement. whilst also offering them a safer and more secure environment.

3. Microsoft Teams allows virtual collaboration and communication which reduces the requirement to travel or attend external meetings. Whilst also offering staff a safer and more secure environment.

STEP 3: Consultation process

Consider how to consult with relevant stakeholders:

1. Describe when and how you will seek individuals' views or justify why it's not appropriate to do so?

2. Who else do you need to involve within your organisation?

3. Do you need to ask your processors to assist?

4. Do you plan to consult information security experts or any other experts?

1. This is not relevant

2. The Systems and Security teams have been involved in implementation.

3. We did not require the assistance of any processors. Microsoft is a data processor, however it wasn't necessary to ask them for assistance with implementation, as Teams is a platform which we have configured for our individual requirements

4. In consultation with the Information Security team, a Risk Assessment Report. has been completed

STEP 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

1. What is your lawful basis for processing?

2. Does the processing actually achieve your purpose?

3. Is there another way to achieve the same outcome?

4. How will you prevent function creep?

5. How will you ensure data quality and data minimisation?

6. What information will you give individuals?

7. How will you help to support their rights?

8. What measures do you take to ensure processors comply?

9. How do you safeguard any international transfers?

1. Consent, Public task, Contract

2.Yes

3.No

4. Not relevant to Microsoft Teams.

5. Not relevant to Microsoft Teams.

6. Not applicable.

7. Not applicable.

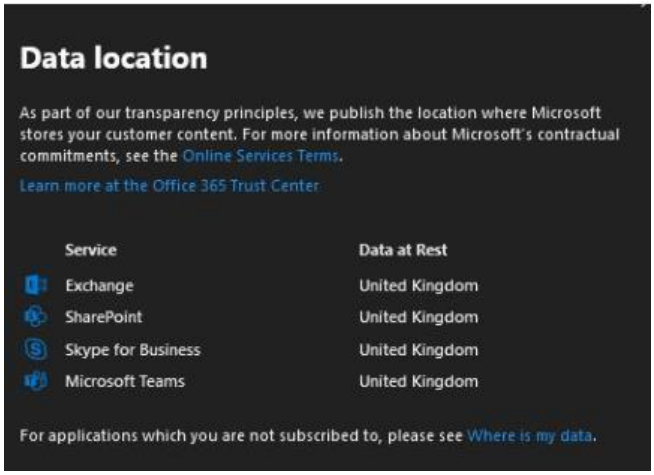
8. Microsoft has different tiers of certification compliance that are labelled as A,B,C,D.

A	B	C	D
Microsoft Cloud Services[1] Privacy and Security commitments	Microsoft Cloud Services Verified with International standards and terms	Microsoft Cloud Services Verified with International and Regional standards and terms	Microsoft Cloud Services Verified with International, Regional and Industry specific standards and terms
Strong Privacy and Security Commitments • No mining of customer data for advertising • No voluntary disclosure of customer data to law enforcement agencies • General Privacy and Security Terms of the Online Services Terms • FERPA	Strong Privacy and Security Commitments • ISO 27001 • ISO 27018 • EU Model Clauses (EUMC) • HIPAA Business Associate Agreement • Commitments included in Tier A	Strong Privacy and Security Commitments • SSAE 18 SOC 1 Report • SSAE 18 SOC 2 Report • Commitments included in Tiers A-B Contractual commitment to meet US and EU customer data residency requirements	Strong Privacy and Security Commitments • FedRAMP • IRS 1075 • FFIEC • HITRUST CSF Assurance Program Assessment • CSA STAR Self-Assessment • Australia IRAP • FISC (Japan) • Commitments included in Tiers A-C
Admin controls are available to enable or disable services in this tier	Admin controls are available to enable or disable services in this tier	Services in this tier may be enabled by default	Services in this tier are enabled by default

A	B	C	D
– Outlook Mobile for iOS and Android – Sunrise for iOS and Android –	– Workplace Analytics	– Azure Information Protection – Bookings – Flow – Kaizala[2] – Microsoft Dynamics 365 – Microsoft Forms – Microsoft Intune – Microsoft StaffHub – Microsoft To-Do for Web – Microsoft Whiteboard – MyAnalytics – Office 365 Video – Planner – Power Apps – Sway – Yammer Enterprise – Office 365 Cloud App Security	Office 365 for Enterprise, Education and Government plans that include – Access Online – Azure Active Directory – Exchange Online – Exchange Online Protection[3] – Microsoft Teams – Office 365 ProPlus[4] – Office Delve – Office Online – OneDrive for Business – Power BI – Power BI for Office 365 – Project Online – SharePoint Online – Skype for Business Online – Microsoft Stream

Tier D has strictest of requirements meeting the commitments listed in tiers A-D. Microsoft Teams and all the related services are tier D compliant. In addition, teams is backed by Azure AD which offers security controls such as single sign on and two factor authentication.

9. Teams data resides in the assigned geographic region of Azure cloud infrastructure depending on the organisations Office365 tenant. In our case the servers are based UK.



Data location

As part of our transparency principles, we publish the location where Microsoft stores your customer content. For more information about Microsoft's contractual commitments, see the Online Services Terms.

Learn more at the Office 365 Trust Center

Service	Data at Rest
Exchange	United Kingdom
SharePoint	United Kingdom
Skype for Business	United Kingdom
Microsoft Teams	United Kingdom

For applications which you are not subscribed to, please see Where is my data.

STEP 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	**Likelihood of harm** Remote, Possible or Probable	**Severity of harm** Minimal, Significant, or Severe	**Overall risk** Low, Medium or High
NHS CFA Privileged & Standard User – As a result of negligence or malicious intent, data could be stolen/modified.	Remote	Minimal	Low
Data Centre Staff (Non-Admins) – As a result of theft or accidental damage to the server hosting the components.	Remote	Minimal	Low
Physical Intruder to Data Centre - In the event of physical intruder the system could suffer from a denial of service due to damage or theft.	Remote	Severe	Medium
Environmental Disaster – Due to an unforeseen disaster, be it intentional (Arson) or a natural disaster (Flood, Fire), the server could be damaged or destroyed. This would result in a denial of service for this system and data loss.	Remote	Severe	Medium
Accidental Screen & File sharing – Teams members could share a screen / file accidentally not intended to the recipient.	Remote	Significant	Medium
Internet Attackers - As a result of a successful compromise of the Microsoft network by an attacker originating from the internet, there is a risk that they could gain access to servers hosting the Teams servers or components of the Teams servers, which may result in a loss of data/denial of services. However we are not permitting the sharing of official sensitive documents.	Remote	Significant	Medium

STEP 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.	Effect on risk Eliminated, Reduced, Accepted	Residual risk Low, Medium, High	Measure approved Yes/No
Continual assessment of opportunities to improve network security.	Reduced	Medium	
Continual monitoring of access rights given to staff and removal of access where it is no longer required.	Reduced	Medium	
Physical Intruder to data centre is out of our control and therefore the risk has been mitigated as much as possible	Reduced	Medium	
Environmental disaster is out of our control and therefore the risk has been mitigated as much as possible	Accept	High	
Accidental Screen and File Sharing – staff have been made aware not to share official sensitive documents.	Reduced	Medium	
Internet Attackers – this is out of our control as the data centre is not exclusive to NHSCFA. As such the risk has been mitigated as much as possible.	Reduced	Medium	

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before proceeding.
DPO advice provided		DPO should advise on compliance, step 6 measures and whether processing can proceed.
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' view, you must explain your reasons
Comments: Having reviewed the DPIA I am satisfied that a comprehensive assessment of the platform has been undertaken. The use and sharing of special category (sensitive) and criminal convictions data on the platform is prohibited. Use of the platform will be controlled by IT administrator with staff use and access to the platform is linked to their user accounts and therefore will be fully auditable. All data will be held in accordance with current data legislative requirements and handled in accordance with organisational best practice and its data retention policy. I am therefore satisfied with the organisational security measures in place.		
This DPIA will be kept under review by:	Trevor Duplessis 18th September 2020	The DPO should also review ongoing compliance with DPIA

Ownership

16. The following table describes the roles and responsibilities:

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	NHSCFA Corporate Information Asset Owners
Senior Information Risk Owner (SIRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	Information Systems and Security
Data Protection Officer	Trevor Duplessis Information Governance and Risk Management Lead

2. DPIA Report

Section 1: Overview of Data Collection and Maintenance

1. Microsoft Teams is chat based collaboration platform complete with document sharing, online meetings and many useful features for business communication. Having a team space is a key to make creative decisions and communicate with members who might be spread across the globe.

2. Microsoft processes data as part of the service offering. The data includes
    - **Content:** Meetings and conversations chats, voicemail, shared files, recordings and transcriptions. Sharing of documents is controlled by the person sharing, and the persons receiving could not save to their own file. In addition to this, staff were made aware in the Teams guidance, that the content should not include special category or criminal convictions data. This will be reiterated and made explicitly clear via regular updates through publication channels such as the staff intranet Go2
    - **Profile Data:** Data that is shared within your company about you. Examples include your E-mail address, profile picture, and phone number.
    - **Call History:** A detailed history of the phone calls you make, which allows you to go back and review your own call records.
    - **Call Quality data:** Details of meetings and call data are available to your system administrators. This allows your administrators to diagnose issues related to poor call quality and service usage.
    - **Support/Feedback data:** Information related to troubleshooting tickets or feedback submission to Microsoft.
    - **Diagnostic and service data:** Diagnostic data related to service usage. This personal data allows Microsoft to deliver the service (troubleshoot, secure and update the product and monitor performance) as well as perform some internal business operations, such as:

3. The impact level of Microsoft Teams was assessed as CONFIDENTIAL and it can only be accessed internally.

4. The following measures briefly describe what controls have been implemented to protect the platform and the personal data recorded:

a. The Platform is accessed by all members of staff from NHSCFA, which includes 3 teams service administrators

b. The platform does not have any direct interconnections with other NHSCFA systems and applications. But the data is stored in different places as mentioned in the Data Entity Storage diagram above.

c. The Data Custodian must comply with the data protection requirements Examples include: regularly reviewing the business requirement to record the personal data; ensuring that the data is not excessive; it is being used for the purpose intended; that there is a deletion and disposal policy; that the application is registered on the NHSCFA register and the NHSCFA DPO is aware of its existence.

5. It is assessed that there are no residual privacy risks to personal data used by Microsoft Teams

6. This DPIA must be reviewed if any changes are made to the personal information if used by the database or any other changes are made that affect the privacy of an individual.

Section 2: Uses of the Application and the Data

7. The purpose of the platform is to allow improved communication and collaboration.

8. Administration of the platform will be the responsibility of Information Systems and Security

9. Information in the platform could include;

- 1-1 Chats
- Channel Messages
- Files Shared, however we are not permitting the sharing of official sensitive documents.
- Recorded meetings

10. The platform does not include processing of any sensitive data, as stipulated in the Teams guidance that there should be no sharing of official sensitive documents.

11. The IAO must comply with data protection requirements. Examples include: regularly reviewing the business requirement to use the personal data; ensuring that the data is not excessive, it is being used for the purpose intended; that there is a deleting and disposal policy; that the application is registered and the DPO is aware of its existence.

Section 3: Data Retention

12. The platform is subject to NHSCFA Data Handling and Storage Policy

Microsoft Teams uses

Chats – The policy applied is retention and deletion. Retained for 180 days and then deleted automatically. There are no paper records. The same doesn't apply to recordings. The recording is stored indefinitely in the folder belonging the person who records, and it is up to them when they delete the recording. This will be covered in a separate DPIA for Microsoft Stream

13. The IAO is required to review the retention period and any requirement to change must be submitted to the Senior Information Risk Owner.

Section 4: Internal Sharing and Disclosure of Data

14. All NHSCFA staff have access to the platform, however administrative access is restricted to only 3 database administrators.

Section 5: External Sharing and Disclosure of Data

15. As the data saved in Teams is in relation to chats, there would be no information of relevance to share with external organisations. File sharing will be covered in a separate DPIA for SharePoint and One Drive. However there are currently no permissions to allow external sharing.

Section 6: Notice/Signage

16. NHSCFA's privacy policy on its website hosts separate sections in relation to data collection, retention and storage. This broadly covers all elements of the NHSCFA usage of data, in a nonspecific manner.

17. The use of signage or other notifications to notify the public of the gathering and use of personal data is not relevant to this platform and therefore outside the scope of this DPIA.

Section 7: Rights of Individuals to Access, Redress and Correct Data

18. Individuals subject to certain exemptions, have the right to gain access to their own personal data. In the event an access request is directly or indirectly received by NHSCFA, we are required to provide the individual who has made the request with details of the personal data recorded about them.

19. It is unlikely that any access requests will be received as the data recorded is from the content of internal chats

20. In the unlikely event that information is identified as being incorrect, NHSCFA staff will take appropriate steps to correct the record where permissible.

21. All NHS employees and member of the public have the right to access, redress and correct personal data recorded about them.

Section 8: Technical Access and Security

22. The security and technical access architecture of the Database/System is as explained in this DPIA:

23. Access is restricted to internal staff only.

Section 9: Technology

24. The platform holds personal information saved from internal chats and is located in the NHS Counter Fraud Authority tenant hosted in Microsoft Azure Infrastructure.

3. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that Microsoft Teams, and any personal data that it records, and its business activities, are compliant and maintain compliance with:

   a. The GDPR and the Data Protection Act in general;

   b. The Data Protection Principles;

   c. The interpretations of the Principles.

2. **This is not a recommendation but a requirement of law.**

3. The roles and responsibilities for the protection of personal data are described in the NHSCFA security policy.

The Privacy and Electronic Communications Regulations

4. The Privacy and Electronic Communications Regulations is not applicable as personal data is not exchanged with external organisations for commercial purposes.

The Human Rights Act

5. The decisions and activities of the organisation are undertaken in compliance with the Human Rights Act, having due regard to appropriateness and proportionality to ensure compatibility with Convention rights.

The Freedom of Information Act

6. As a public authority we are compliant with the provisions of the Freedom of Information Act, in proactively publishing and making available upon request, certain recorded information held by the organisation subject to any relevant exemption(s). However, no personal information would be disclosed under the Freedom of Information Act as this would breach the data protection principles.

Conclusion

7. There are no residual privacy risks to the personal data recorded in the platform. The controls described in this DPIA explain in detail how the data is protected and managed in accordance with the GDPR and Data Protection Act 2018. The DPO is responsible for ensuring that the controls are implemented through the life cycle of the system.

Annex A - Definition of Protected Personal Data

Personal data includes all data falling into Categories A, B or C below:-

A. Information that can be used to identify a living person, including:

Name;
Address;
Date of birth;
Telephone number;
Photograph, etc.

Note: this is not an exhaustive list.

B. Information which, if subject to unauthorised release, could cause harm or distress to an individual, including:

Financial details e.g. bank account or credit card details;
National Insurance number;
Passport number;
Tax, benefit or pension records;
DNA or fingerprints;
Travel details (for example, at immigration control or oyster records);
Place of work;
School attendance/records;
Material related to social services (including child protection) or housing casework.

Note: this is not an exhaustive list.

C. Sensitive personal data relating to an identifiable living individual, consisting of:

Racial or ethnic origin;
Political opinions;
Religious or other beliefs;
Trade union membership;
Physical or mental health or condition;
Sexual life
Commission or alleged commission of offences;
Proceedings relating to an actual or alleged offence.

Any data set containing this information must be processed in accordance with the GDPR and the Data Protection Act 2018 (DPA 2018).

Particular care must be taken with data in Category B and with any large data set. Information on smaller numbers of individuals may justify additional protection because of the nature of the individuals, source of the information, or extent of information.

There are additional, specific constraints within the provisions of GDPR and the DPA (2018) on the processing of data in Category C.

Annex B - Data Protection Compliance Check Sheet

PART 1: BASIC INFORMATION - New or existing Project, System, Technology or Legislation

1. Organisation and project.

Organisation	NHSCFA
Branch / Division	NHSCFA – ISA
Project	Microsoft Teams

2. Contact position and/or name
(This should be the name of the individual most qualified to respond to questions regarding the DPIA)

Name, Title	Trevor Duplessis
Branch / Division	Finance and Corporate Governance, NHSCFA

3. Description of the programme / system / technology / legislation (initiative) being assessed.
(Please note here if the initiative does not collect, use or disclose personal data*). If this is a change to an existing project, system, technology or legislation, describe the current system or program and the proposed changes.

Microsoft Teams is a unified communications and collaboration platform with document sharing, online meetings and many more useful features for business communications. It is part of the Microsoft 365 suite of applications designed to simplify group work

4. Purpose / objectives of the initiative (if statutory, provide citation).

NHSCFA leads on a wide range of work to protect NHS staff from economic crime.

Teams is an office productivity tool used mainly for communication between people and exchanging messages in a channel as part of a project or group activity. Teams has 3 main features

Chat – Chat with anyone in the organisation and all the conversations are searchable.

Conferencing – Conduct online meetings and video calls which includes screen sharing.

Collaboration – Integrates with different business applications from third party providers

5. What are the potential privacy impacts of this proposal?

Data Protection Impact Assessments (DPIA) have been considered in the light of personal data gathered, and the data in Microsoft Teams has been gathered for a specific, justifiable and proportional purpose and found to be mitigated by the steps put in place to minimise the possibility of unauthorised access or use (see Compliance Checks in section 3 of this document)

6. Provide details of any previous DPIA or other form of personal data* assessment done on this initiative (in whole or in part).

This is the first DPIA carried out on the system

IF THERE IS NO PERSONAL DATA INVOLVED, GO TO PART 3: DPA COMPLIANCE - CONCLUSIONS

*IMPORTANT NOTE: 'Personal data' means data which relate to a living individual who can be identified: (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Page left intentionally blank.

NHSCFA offices

Coventry

Earlsdon Park
55 Butts Road
Coventry
West Midlands
CV1 3BH

London

4th Floor
Skipton House
80 London Road
London
SE1 6LH

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH