NHS
Counter Fraud Authority

Microsoft Stream – Cloud Based Platform

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 Microsoft Stream.

Microsoft Stream is an Enterprise Video service where people in the organisation can upload, view, and share videos securely. One can share recordings of meetings, presentations, training sessions, or other videos that aid in a team's collaboration.

Stream provides the following product capabilities in a standalone product or as part of Microsoft Office 365 enterprise subscription:

Video upload and metadata editing: Stream's input of video file types is limited to formats supported by Azure Media Services. Users can upload video files individually or in bulk. Once uploaded, the file owner can make changes to file name/ title, add a description, choose a thumbnail, assign hashtags or upload caption files. Standalone Video can also be uploaded but it will be only available with the owner unless he shares it with someone internally. This functionality is available to everyone. If we restrict uploading standalone videos, it will apply to all meeting recordings via teams as they won't get stored in Stream but will be available in Teams Chat Window for 20 days.

Video playback on internal sites: Once the videos are automatically transcoded for playback on all devices, users can watch the videos within the Stream portal, or embed them on other company sites. However, it must be noted that Stream does not support external stakeholder access and only allows authorized active directory users to access the videos, whether they are embedded on other organisational sites or played within Microsoft Stream.

Video sharing within the organisation: Stream allows video owners to share and assign videos to one or multiple channels, a custom group of viewers, or make the videos private. The video files can only be shared within the company via a link, email or an embed code, which displays the content on other organisational platforms.

Organising videos: Stream enables users to create channels to organise videos by topics or other categories. Channel creation and content contribution can be restricted to an authorised list of users. Videos can also be organised in mini-group portals, only available to authorized group members. Groups also contain channels for further categorization of content.

Intelligent video search: Microsoft Stream features a range of intelligent features that improve content searchability within the portal. All videos are supported with speech to text transcription, which becomes searchable text that helps users jump to any spoken word in the video.

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'**

Nothing contained herein should be construed as endorsing any particular Technical Solution to any United Kingdom Government Invitation to Tender.

Table of contents

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

Prefix	
Reference:	**DPIA Microsoft Stream**
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

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 effect 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:

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:

use new technologies;

match data or combine datasets from different sources;

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.

[1] GDPR - Recital 75

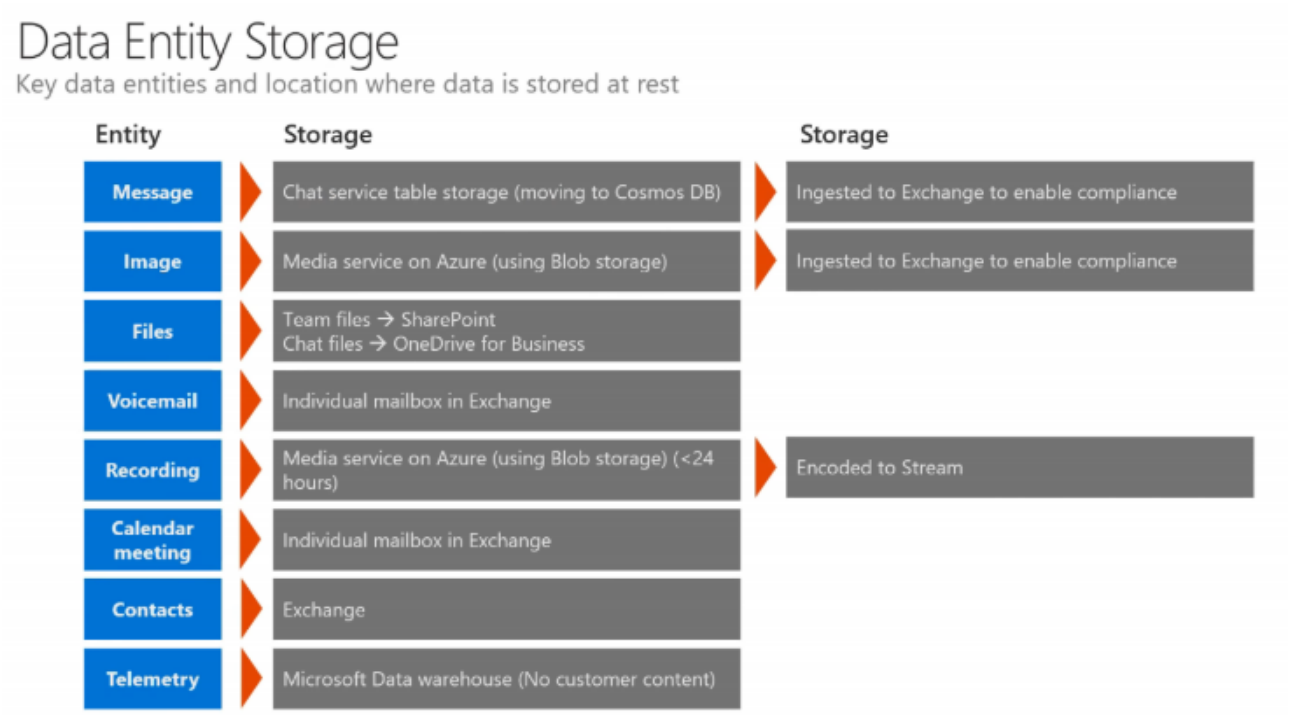
8. Conducting a DPIA is a legal requirement for any type of processing. Failure to carry out a DPIA in required cases may leave the organisation open to enforcement action, including a **fine of up to €10 million**.

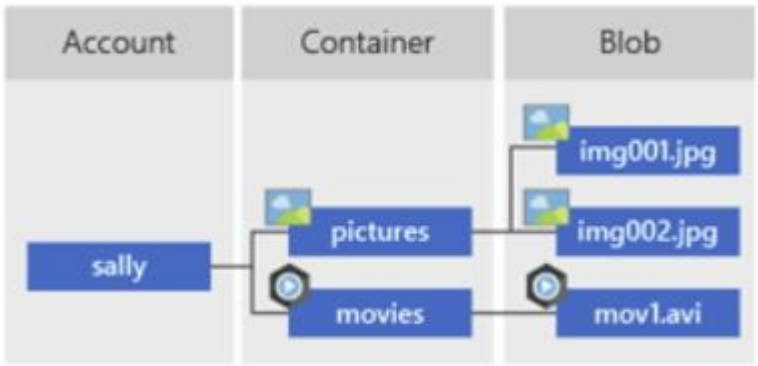
9. This DPIA is related to the NHSCFA Risk Assessments, which outline the threats and risks. The Risk Assessment document was developed in accordance with the requirements of NHSCFA and CESG HMG Infosec Standards 1 and 2

Microsoft Stream General Description

10. Microsoft Stream, a Microsoft Azure Cloud solution, allows enterprise users to upload, manage and share videos within their organisation. Users simply sign up using their business email (active directory integration), invite co-workers to join, and start uploading and sharing video content.

11. Microsoft stores different kinds of data in different kinds of services or applications. The Data Entity Storage model below shows where Microsoft Stream stores its different data.
Azure Blob storage is used behind the scenes of the Azure Platform, and provides scalable, cost-efficient object storage in the cloud. It allows to store large amounts of unstructured data like audio, video images etc. Blob storage hierarchy consists of Storage Account - > Containers -> Blobs. Please see images below:





12. The platform is accessed by all members of staff from NHSCFA, which includes 4 Stream administrators. However, by default the recorder will be the owner of the video and the participants are the members. Owners and administrators can edit the permissions, delete the video, and download to personal drives. If it is shared within Stream to other members, they can only view and share.

13. This is the only DPIA to be completed on Microsoft Stream 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.

14. 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

15. 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:

Step 1 - Identify the need for a DPIA

Step 2 - Describe the processing

Step 3 - Consultation process

Step 4 - Assess necessity and proportionality

Step 5 - Identify and assess risks

Step 6 - Identify measures to reduce risk

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.
As mentioned above Microsoft Stream is an Enterprise Secure Video service where people in the organisation can upload, view, and share videos securely. One can share recordings of meetings, presentations, training sessions, or other videos that aid in a team's collaboration. Microsoft Stream has the ability to manage restrictions on access via identity management system Azure Active Directory. It's a highly adaptive platform, allowing you to use it for general internal communications as well as live online training sessions. It's integrated into a host of Microsoft 365 enterprise products such as Microsoft Teams (Meeting Recordings, Live Event Recordings), SharePoint, OneNote etc to make it easy to share content or invite colleagues to participate across different channel options. Processing involves audio and video files, which can include the recording of personal imagery and audio - individuals faces and voices. **Note : Microsoft is rebuilding its Microsoft Stream video service over the next several months and will be moving it to use SharePoint Online and OneDrive for Business for storing and managing videos across Microsoft 365. This will be a move from the current Microsoft Stream Classic to a new Microsoft Stream. (Q2 2021)**

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. Recordings are stored in Microsoft Stream with the person responsible as the owner of the video who initiated the recording. Communications will be circulated to explain that it is the responsibility of the owner to ensure deletion, and that Stream administrators are only there to step in if someone leaves the organisation without deleting their videos.

By default, the recorder will be the owner of the video and the participants are the members. Owners and Administrators can edit the permissions, delete the video, etc. Members can only view and share the video.

Stream Administrators can:

1. edit the video permissions like the owner of the video.
2. see all the videos irrespective of video visibility through admin mode.
3. recover the deleted videos in the recycle bin, if needed.

2.Source of the data is communications such meetings, live events among staff used for official business purposes, and although personal communication is permitted this should be limited.

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 video 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 Microsoft Stream servers or components of the Stream servers, which may result in a loss of data/denial of services.

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? 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 video/audio communications. It does not include official sensitive, special category or criminal offence data. 2. Data is collected on a continuous basis which applies to all the NHSCFA Staff. 3. Data is collected on a continuous basis. 4. Meeting recordings are stored indefinitely in Stream and it is the responsibility of the owner to make sure it is deleted should it not be deemed necessary for official purposes. There are no automated warnings, as the storage space is allocated on tenant basis and then per user. Nearly 500,000 videos can be stored as of now for CFA tenant. Communications will be circulated to explain that it is the responsibility of the owner to ensure deletion, and that Stream administrators are only there to step in if someone leaves the organisation without deleting their videos 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 meeting/live event by the owner of a team.

2. Meeting owner / Live Event Organiser have full control of the video recordings and who it can be shared with.

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 Stream 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 Stream 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 applicable

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 Stream is a platform where recordings get stored.

4. In consultation with the Information Security team, a Risk Assessment Report has been completed for Office 365 platform.

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 Stream.

5.Data to be kept no longer than necessary in accordance with the Data Retention Schedule

6.Recorded staff will receive a notification on screen to advise they are to be recorded. They then have the option to continue or leave the meeting.

7. Recorded staff will receive a notification on screen to advise they are to be recorded. They then have the option to continue or leave the meeting

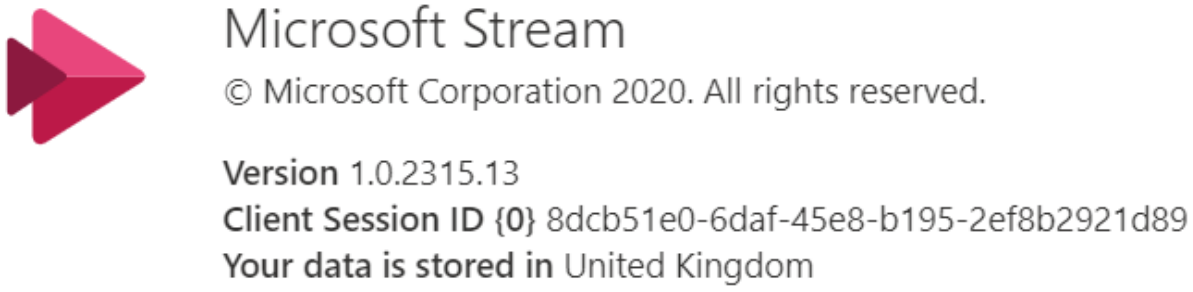
8. Microsoft has different tiers of certification compliance that are labelled as A,B,C,D.

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 Stream and all the related services are tier D compliant. In addition, Stream is backed by Azure AD which offers multi factor authentication.

9. Microsoft Stream 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.



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, video files could be stolen/modified, copied to external medium	Remote	Significant	Medium
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 Audio/Video sharing – Video owners could share 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 audio/video file Sharing – staff have been made aware it is the meeting recording owners responsibility to delete if it is not required for any business purposes. Staff have also been made aware not to share official sensitive documents, via circulation of the 'Teams End User Guide' (appended in Annex C)	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: Having reviewed the DPIA I am satisfied that a comprehensive assessment of the platform has been carried out. The use and sharing of special category (sensitive) and criminal convictions data on the platform is prohibited. Use of the platform will be controlled and overseen by the IT administrators with staff use and access to platform linked to their user accounts and will therefore be fully auditable. All data will be held and governed in accordance with current legislative requirements and handled in accordance with organisational best practice and its data retention policy. I am therefore satisfied with the with the organisational security measures employed.		
DPO advice accepted or overruled by:	Trevor Duplessis - 27th October 2020	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:		
This DPIA will be kept under review by:		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 Stream is the video management and sharing service for employees at all levels across businesses of all sizes who are interested in using videos in the workplace to connect, collaborate, learn and share information. Anyone can search for videos easily and consume them on their device, whenever and wherever.

2. A brief overview of the data contained within the platform is:
Video Recordings – Teams Meetings, Live Events, Training Sessions, Corporate Presentations

3. The impact level of Microsoft Stream was assessed as **OFFICIAL** and it can be accessed internally on the NHSCFA network and on the web.

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 4 Stream administrators. However, by default the recorder will be the owner of the video and the participants are the members. Owners and administrators can edit the permissions, delete the video, etc. Members can only view and share the video.

    b. The platform does not have any direct interconnections with other NHSCFA systems and applications

    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 the personal data used by the platform

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 Database/System could include:
Audio/Video Recordings of Meetings, Live Events, Training, Corporate Presentations

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 measures that have been implemented to protect the Personal Data are:

a. The platform is accessed by all members of staff from NHSCFA, which includes 4 Stream administrators However by default the recorder will be the owner of the video and the participants are the members. Owners and administrators can edit the permissions, delete the video, etc. Members can only view and share the video.

b. The platform does not have a direct interconnection with other NHSCFA systems or applications

c. 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 Stream data is stored indefinitely, and in accordance with the Data Retention Schedule, the responsibility lies with the owner of the video to make sure they delete it if is no longer required for any business purposes.

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 including Stream administrators.

Section 5: External Sharing and Disclosure of Data

15. External sharing of data is not allowed in Stream.

Section 6: Notice/Signage

16. Meeting attendees have the ability to use the recording feature in Teams which is subsequently stored in Stream. However, once the feature is activated, other meeting participants would receive notification of the intention to record, allowing them the option to decline the recording and exit the meeting.

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 many access requests will be received as the personal data recorded is all in relation to internal meetings and presentations.

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 platform is as explained in this DPIA:

23. Access is restricted to internal staff only.

Section 9: Technology

24. The platform holds official information saved from recorded meetings 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 the Microsoft Exchange-Outlook, and the 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 Stream

2. Contact position and/or name, telephone number and e-mail address.
(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 Stream is an Enterprise Video service where people in the organisation can upload, view, and share videos securely. One can share recordings of meetings, presentations, training sessions, or other videos that aid in a team's collaboration.

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.

The purpose of the platform is to aid in collaboration among peers.

Access is restricted to members of staff within NHSCFA, including the Stream administrators.

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 Stream 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 platform

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

NHS
Counter Fraud Authority

Annex C: Appended - Microsoft Teams End User Guide

Microsoft Teams

End User Guide

June 2020

Version 1.1

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

Document Control

Document Reference	Microsoft Teams – End User Guide
Document Location	NHSCFA Intranet
Title	Microsoft Teams – End User Guide
Author	Security and Operational Support Analyst
Release Date	18th June 2020
Issued To	ISA
Status	Initial release

Review History

Version Reviewed	Review Date	Reviewer	New version	Comments

Version History

New Version	Review Date	Author	Details of Amendments
1.0	N/A	ISA	Initial Release version
1.1	N/A	ISA	Updated

Table of contents

Introduction

This document will attempt to provide a summary and overview of Microsoft Teams. This will cover what Microsoft Teams is, why we are using it and, most importantly how to use it effectively and securely.

What is Microsoft Teams?

Microsoft Teams is a unified communication and collaboration platform that combines persistent workplace chat, voice and video meetings with file sharing and other functionality. It is Microsoft's replacement for Skype for Business and is the NHSCFA's replacement for Notes SameTime. Teams makes it possible to share files and collaborate on documents between Team members and can be used to communicate with anyone within the NHSCFA as well as certain external parties.

As this is a new application to the NHSCFA, some functionality has not been enabled and some integrated functions are still under investigation, development and configuration. Therefore, we have compiled the list below to give you an idea of what you can and cannot or should not use at this stage.

TEAMS is still under development by Microsoft and things change, often quite quickly. New features are added, and elements of the interface can change, even as they have done during the creation of this document.

This user guide will be updated as additional functionality is investigated, securely configured and approved for use.

What can and can't I do in Teams NOW?

You CAN use from the start:

Instant messaging with internal staff

Calls - voice and video, including team meetings.

Communication with external partners/attendees – can be invited to meetings by email

Screen sharing

Live Events/Town Hall meetings – Available very shortly but access will be restricted

Recording Live Events (Please ask for advice)

Please DO NOT use or request the following yet:

File upload/sharing – please do NOT use this until notified by ISA

Recording calls or meetings other than Live Events

Guest access to your TEAMs for non-NHSCFA users

One Drive - This is linked to file sharing/uploading, so please do NOT use this yet.

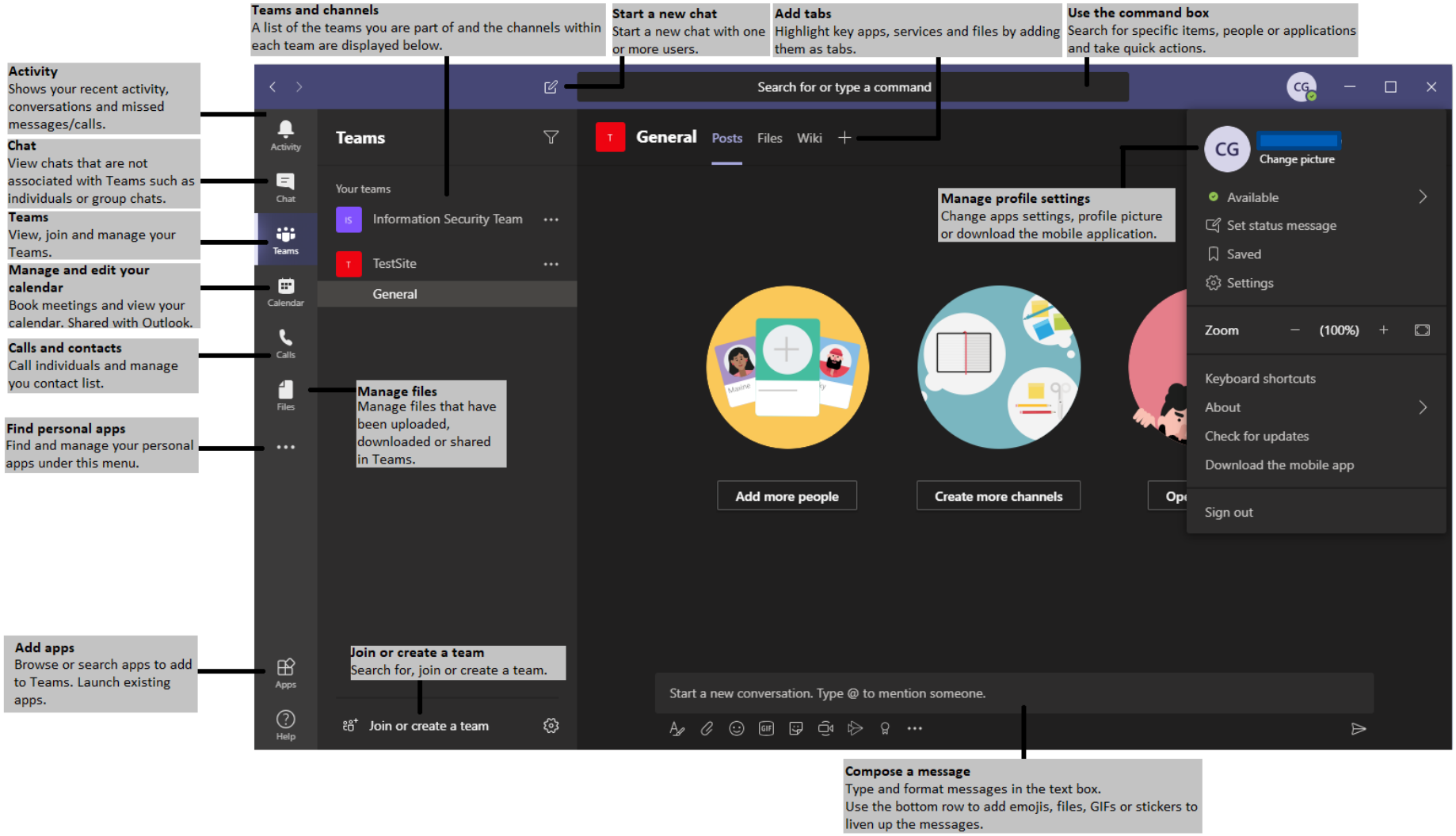
Teams Apps - May be made available later but only on request.

How do I access Teams?

Teams can be accessed in two ways. The usual method is to use the Teams application (App), the main focus of this guide. The other is via the Teams web application.

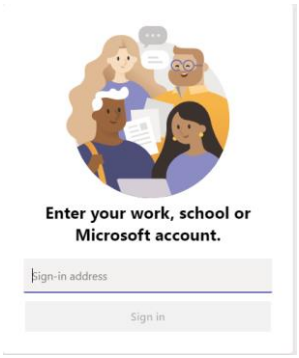
While working remotely, away from NHSCFA sites, we strongly advise you run Teams on the computer you are physically using, not on a remote computer. While remote computers will pick up keyboard and mouse inputs, they will not pick up audio or video inputs and you will not be able to be heard or seen if using video.

On the next page is an example of the Teams interface with annotations of some key features.


Teams and channels
A list of the teams you are part of and the channels within each team are displayed below.
Start a new chat
Start a new chat with one or more users.
Add tabs
Highlight key apps, services and files by adding them as tabs.
Use the command box
Search for specific items, people or applications and take quick actions.
Activity
Shows your recent activity, conversations and missed messages/calls.
Chat
View chats that are not associated with Teams such as individuals or group chats.
Teams
View, join and manage your Teams.
Manage and edit your calendar
Book meetings and view your calendar. Shared with Outlook.
Calls and contacts
Call individuals and manage you contact list.
Manage files
Manage files that have been uploaded, downloaded or shared in Teams.
Find personal apps
Find and manage your personal apps under this menu.
Add apps
Browse or search apps to add to Teams. Launch existing apps.
Join or create a team
Search for, join or create a team.
Search for or type a command
Teams
Activity
Chat
Teams
Calendar
Calls
Files
Apps
Help
Your teams
Information Security Team
TestSite
General
General
Posts
Files
Wiki
Manage profile settings
Change apps settings, profile picture or download the mobile application.
CG
Change picture
Available
Set status message
Saved
Settings
Zoom
(100%)
Keyboard shortcuts
About
Check for updates
Download the mobile app
Sign out
Add more people
Create more channels
Join or create a team
Start a new conversation. Type @ to mention someone.
Compose a message
Type and format messages in the text box.
Use the bottom row to add emojis, files, GIFs or stickers to liven up the messages.

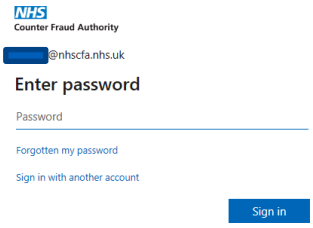
Logging in to TEAMs

In most situations you will not be prompted to login to Teams on your laptop as it uses your Windows account credentials automatically. However, there may be occasions when this doesn't work. If this happens, you will see the following when you launch Teams:



In the "sign in address" box, enter your windows logon ID followed by *@nhscfa.nhs.uk. e.g.*

You will then be presented with the following screen:



Enter your Windows password and click the sign in button. If you have forgotten your Windows password then **do not** click *Forgotten my password* and instead contact the NHSCFA Service Desk.

Teams structure

The TEAMS application uses a concept of Teams and Channels. There may be one or many Channels within a Team.

There are two basic types of users within a Team, Owners and Members. Owners have additional permissions over members.

A number of Teams have been created reflecting the structure of the organisation and some of the permanent working groups.

You will be a member of more than one Team.

What are Channels?

Channels are areas within a Team that can be dedicated to specific topics or for sub-groups of the main team. Each Team has a ‘General’ channel by default and others can be created for Team projects, BAU work, events or whatever purpose is seen as useful to the running of the TEAM. There are two types of channel: public and private.

Public Channels

4. Are accessible to all members of a Team.
5. The General channel is public by default and this cannot be changed.

Private Channels

6. Can only be created by Team owners.
7. Membership is not inherited from the Team but must be granted by a Team owner.
8. Some functionality is restricted in private channels such as One Note and Planner.

Note – Inviting someone to a Team will provide them access to all Public channels in that Team. This should be considered when structuring the channels or a Team as well as when considering inviting someone to a Team.

Each Team contains at least one Channel, named “General” which can currently be used for team communications, text, voice or video. Additional channels can be created within a Team by a Team’s owners and members to fit the CFA Unit’s internal structure and to suit the working practices of that team.

Communications using messages, voice and video can be within a Team using a Channel, or privately, outside the formal Team structure.

Instant Messaging, Voice and Video Calling

Chats vs Conversations

Microsoft's Teams documentation describes two types of instant text-based messaging: Chats and Conversations.

Chats are between one or more people and occur outside the configured Teams structure. They can be informal or arranged meetings.

Conversations are text-based communications held within Teams Channels. The main features of each are described below.

Chat:

- Can be accessed from the Chat 'tab'
- Is used in meetings held outside a Team channel
- Messages are simple and are independent of each other.
- Can be between one or more users.
- Is the default message type for communications not hosted in channels, i.e. one-to-one or group chats and meetings organised via Outlook or the Teams calendar.
- Is meant to be used as instantaneous/temporary communications.
- Messages are visible only to those involved in that communication.

Conversation:

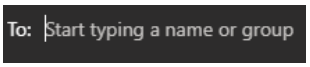
- Communications within Channels in a Team
- Can used as normal messages.
- Can be responded to directly by clicking the Reply button.
- Are visible to all members of the Team or Private Channel.
- Enable collaboration and common messages within a Team Channel
- Meant for long-term use and reference.

Chat (Instant Messaging)

Starting a new Chat

1. In the Teams banner click the **New Chat** icon.

2. In the **To** field, type the name of the person or people you want to chat with.

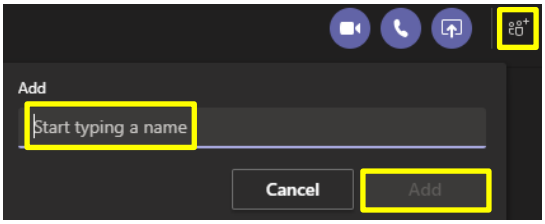


3. In the box where you type your message, type what you'd like to say and click **Send**

Adding people to a Chat

1. To add someone to an existing chat, click the **add people** icon in the top right hand corner of the TEAMs window.

2. In the **Add** field, search for the person or people you would like to invite by typing their name and then click the Add button to invite them into the chat.



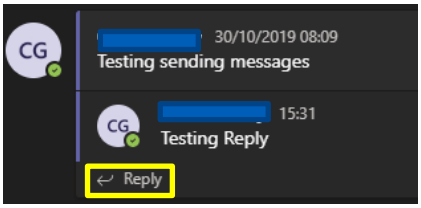
Conversations (Instant messaging in a Team)

Replying to a Conversation

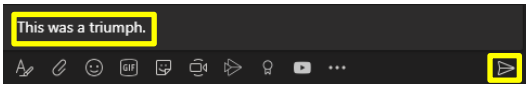
Conversations are series of messages between members of a team or Private channel. They are the similar to a group chat but are retained and visible to all members of that group (Team) even if they are not in attendance when the messages are posted. They form a visible and lasting record of communications within the Team (or channel).

For instance, if a project update were requested, rather than 3 people writing three new messages, they could reply to the request message, thus keeping the information condensed and in one place.

1. Find the conversation thread or message you want to reply to in the appropriate Team Channel.



2. Click **Reply**, add your message and click **Send**.



Note - You cannot add your own emojis to TEAMS, but you can paste pictures into chats from external sources. This has been requested via Microsoft's TEAMs development programme.

NOTE: It is not possible to completely delete a "Chat" or conversation. You can delete your own 'posts' in a conversation but not those of others. All chats are automatically saved by TEAMS and we cannot turn this off!

This means that all chats are available for eDiscovery and are business records, subject to the NHSCFA Information Security, Acceptable Use and other policies.

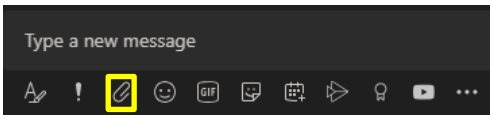
File sharing (upload) in Chat, Conversation or Meeting

NOTE - This has been included in advance of final security and governance configuration so please DO NOT upload files to TEAMS until approval is given to do so by ISA.

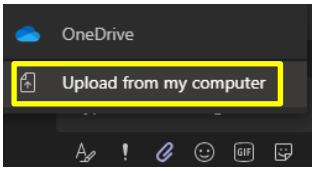
Note – Please carefully consider the sensitivity of the information you share, both internally and externally, and treat TEAMS as similar to standard email. Check the content of any file and if it contains sensitive or Personal Identifiable Information or is marked "OFFICIAL-SENSITIVE" then Do NOT upload it and use alternative, secure ways to share that information!

To upload and share a file with a person, group or TEAM, you follow the same steps for starting a Chat. This section will cover sending it as a regular Chat message and in a Channel Conversation you follow the same process.

1. To send a message to a person or group, open the relevant Chat or Team channel and look at the window at the bottom of the screen.
2. Click on the **Attach** icon 



3. Select the location the file is stored. In this example, it is local.



4. Select the file you would like to send from the dialogue box and click **Open**. Wait for the upload to Teams to complete.
5. Type a message you would like to go with the attachment and click the **Send** button  .

Making Voice and Video Calls

Equipment required to make Voice and Video Calls

1. Work Laptop:

   These have everything you need to make basic voice and video calls. There is a camera at the top of the screen and microphone and speakers are integral to the laptop.

2. Work Desktop:

   You will need additional peripherals to make voice and video calls from an NHSCFA desktop computer.

   For voice calls you will need either an external microphone and possibly speakers, and for video calls you will need a webcam.

   Headsets are preferred in an office environment as they provide some limited privacy and reduce office disruption.

Making a call (Video and Audio)

1. Use the **search** function on the Teams banner to find the person you would like to call and click on the person from the search results

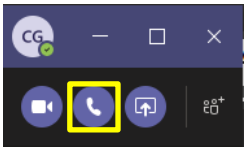
   Or

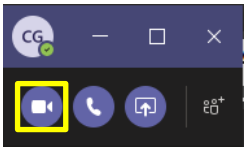
   From an existing **Chat** conversation by clicking the **Chat** option on the left-hand menu and finding the existing chat with the person/s you wish to call.

2. Click the **Phone** icon to make an audio call

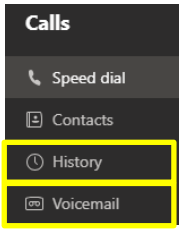
   Or

   Click the **Video** camera icon to make a video call.





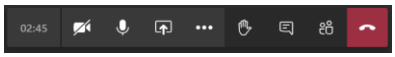
3. View your call history and voicemail, select the relevant option from the left-hand menu.



Note – TEAMs Help and Microsoft documentation online contain information about making external telephone calls using Teams. NHSCFA will not be enabling this functionality.

Switching video and sound on/off and video background effects

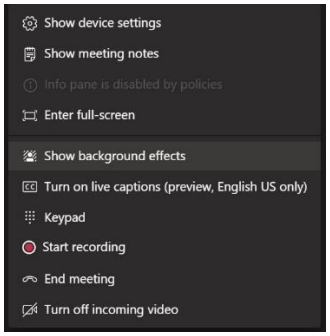
Functionality within a meeting or call is managed using this toolbar:



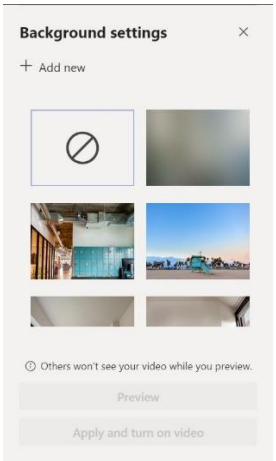
Whilst in a call you can control what functions you use.

1. Audio - by clicking the **Microphone** icon you can mute and re-enable sound.
2. Video – click the **Camera** icon to turn it on and off.
3. You can also select a static background rather than showing your location on screen.

   The change the video background, click on the 3 dots on the toolbar and this will display the following menu of options:



   Selecting “Show background effects” will display the following at the side of the TEAMS windows:



You can select one of the existing stock pictures as your background, including the blurred image shown above.

Alternatively, you can upload and use an image of your choice by clicking “Add new”. This opens a file dialog window where you can select a ‘picture’ file.

At that point, you can either preview the background you have selected, or simply apply it to the current session by clicking ‘Apply and turn on Video”.

Adding people to a call

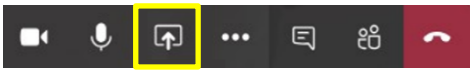
3. To add people to a current voice or video call, click the **View Participants** icon .

4. In the **Invite someone** field, search for the person or people you would like to invite to the call and click to add them.

9.

Screen sharing in a call

1. To share your screen with a person or group from a voice or video call click the **Screen Sharing** icon .



2. Then select what to share with the participant(s).

Note – When selecting what to share, you can select a whole screen, with a choice if you have multiple monitors, or an application window (e.g. Word, Excel, browser). Selection of as desktop screen will show everything on that monitor while selecting an application will only show that application.

Please ensure all applications you do not intend to screen share should be closed or at least minimised before you start the Teams call or meeting.

This is especially important for any application or document with sensitive or PII (Personal Identifiable Information) data and anything marked "OFFICIAL-SENSITIVE". Accidental exposure of such is considered a Data Breach and must be reported to the Service Desk and the Data Protection Officer.

Some examples of information that must NOT be shared using Teams Screen Sharing are SCR records, personnel/HR records, investigation subject data etc.

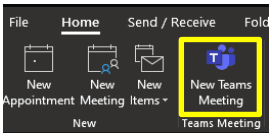
Setting Up Meetings

Creating a Teams meeting from within Outlook

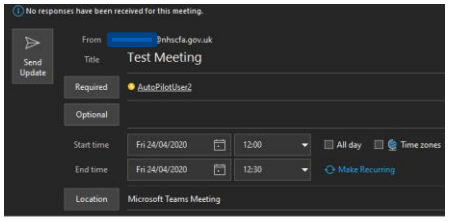
Note – This requires the Teams add-in for Outlook. This should be installed by default, however if you do not see the icon please contact the NHSCFA Service Desk.

1. Open your Calendar in Microsoft Outlook

2. When in **Calendar**, select **New Teams Meeting** from the top menu bar.



3. Clicking **New Teams Meeting** will take you to a screen where you setup a calendar entry as normal. The only difference is that the invite includes a link to a Teams meeting. Enter the details as you normally would. Once done, click **Send**.



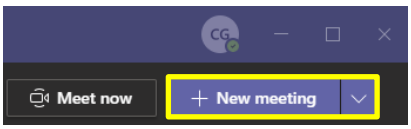
10.

4. To join the Teams meeting, either open the entry in Outlook and click the Teams link or open your calendar in Teams and open the meeting. If you use Outlook it will open a web page, simply allow it to open in the Teams app if prompted or click **Launch it now**.

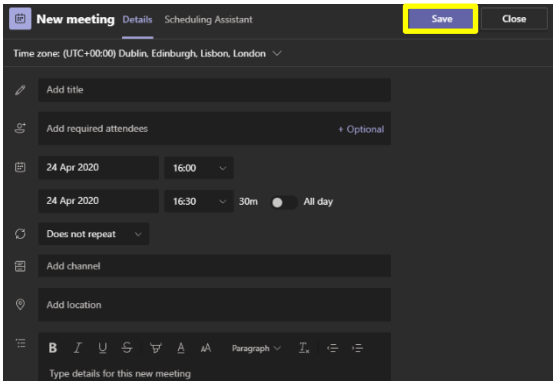
Creating a Meeting within Teams

1. Go to the Teams **Calendar** tab on the toolbar on the left side of the Teams window.

2. Click on the “Meet Now” button to start a meeting immediately or click on “New Meeting to schedule a meeting in the future.



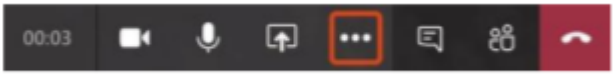
3. Complete the meeting details in the pop-up window. The title names the meeting, the attendees covers who is sent the invitation. The date and time covers when it will occur. The description will inform as to what the meeting is about. Click Save when you are done.



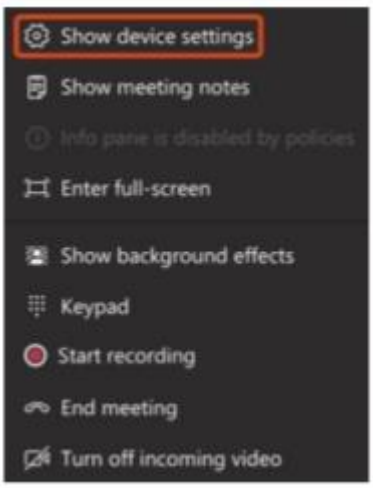
4. To join a TEAMs meeting, go to the Calendar and click the Join button next to the meeting.

Recording in Meeting

1. Inside the meeting window, select the More actions icon (with the three dots)



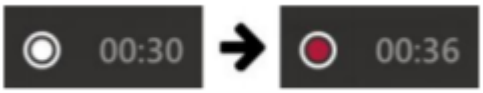
2. Check the volume of your audio by selecting “Show device settings”.



The volume bar will appear which indicates how loud your audio is.

3. When you are ready to record select Start recording from the same menu as mentioned above. Only one person can record the meeting and the person recording is the owner of the video.

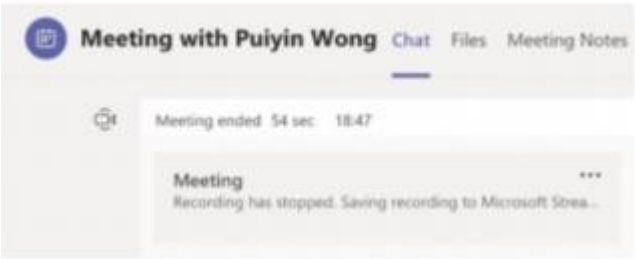
4. After you have selected Start recording there will be white dot icon next to the timer which indicates recording is pending and has not begun. After a few seconds the dot will turn red which indicates recording has begun.



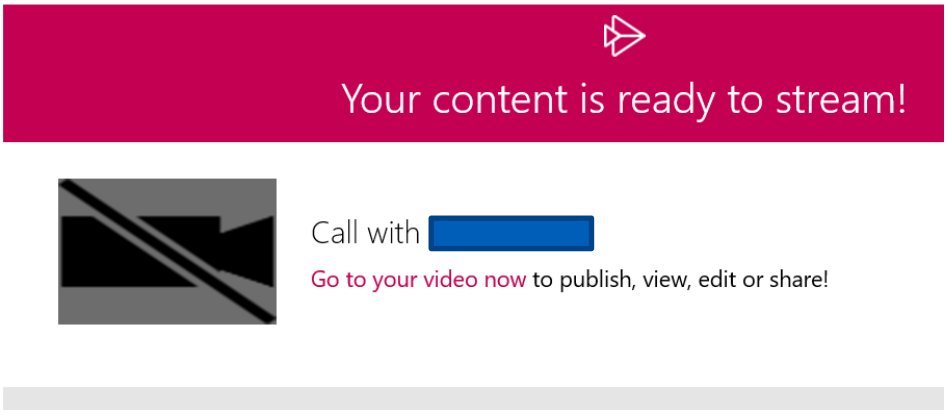
5. You will also be notified with a warning message at the top of the screen.

   “You’re recording. Let everyone know that they’re being recorded”

6. Select Stop recording from the more action’s menu. Recording will be processed and saved to Microsoft Stream. Below status will appear in the chat channel.



7. Recording will be available in the chat window for 20 days. Recording also gets stored in Microsoft Stream. You will receive an email when the content is ready to stream



8. Recordings can be accessed either by clicking on the email link or by going to https://web.microsoftstream.com. Recordings are available indefinitely unless the owner deletes it.

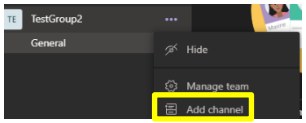
Note : The recordings should be deleted by the owner if there is no purpose / justification to withhold it. Stream administrators can access all the videos.

Working with Teams and Channels

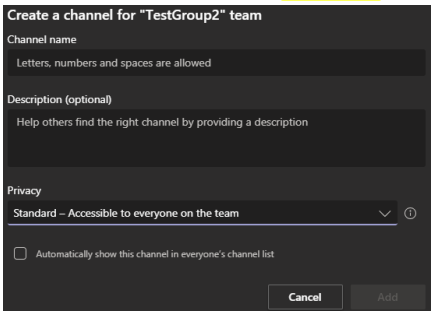
Creating a New Channel

1. From the **Teams** tab.

2. Click on the three dots next to the Team name and select “Add channel” from the drop-down menu.



3. Enter a new **Channel name**, **Description,** if required, and select the appropriate **Privacy** setting, Standard or Private.



Privacy settings allow you to choose who can view a channel. **Standard** channels are accessible to anyone in the **Team** while **Private** channels are restricted to members of a Team added by the Team owner.

If a Standard channel is selected, click **Add**.

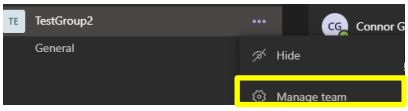
If a Private channel is selected, click **Next**. You will then be prompted to add members to the channel. Follow the on-screen instructions to complete the process.

Note: Only TEAM owners can create Private channels.

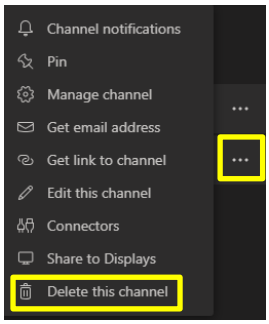
Deleting or removing Channels

1. Go to the **Teams** tab.

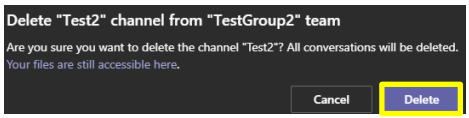
2. Click on the team from which you wish to remove a channel and open it so the Team channels are displayed.



3. Click on the **…** symbol next to the channel you would like to delete and select **Delete this Channel**.



4. Check it is the channel you would like to delete and click the **Delete** button.

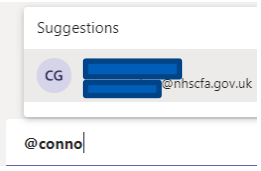


What Other Features Are Available?

@mention someone

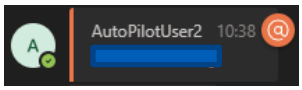
An **@mention** will highlight a message as being directed at a person. Not incredibly useful in a one-on-one chat but it has uses in a larger team chat or group chat.

1. In the chat message box type @ followed by the persons name (it will begin to search for the name after the first few letters).

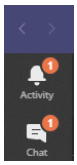


2. Either fill out the name in full or select the user from the menu of the person you would like to **@mention**. This can be done for any number of users

3. Each person who is included will receive a notification in their activity feed. The message will also have an orange @ symbol located next to it.



4. Check for a red circle next to **Activity** to see if you have received an @.

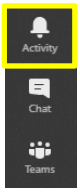


Stay on top of things

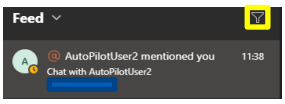
Notifications let you know when someone **@mentions** you, likes something you've posted or replies to a thread you started. The **Activity** feed collects all of this in one area to help you stay on top of it all.

To view your activity feed:

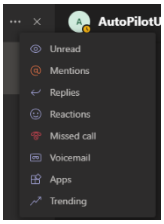
1. Click **Activity**



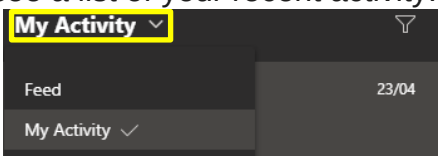
2. You can use the drop down at the top to change between **Feed** and **My Activity**. **Feed** is the default and shows you a summary of everything that's happened in the channels you follow.



3. Click the **Filter** icon to filter the type of activity shown in the **Feed** section.



4. Select the **Feed** drop down and then **My Activity** to see a list of your recent activity.



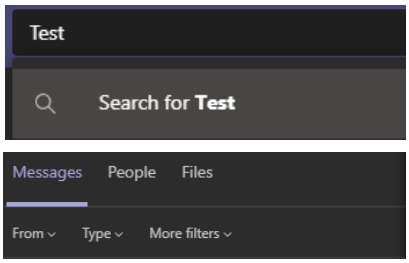
Search for messages and people

Searches cover the entire organisation as well as all of the teams and channels that you're a part of. To carry out a search, follow the below instructions.

Type a phrase in the command box at the top of the application and press Enter.

Select the relevant tab from **People**, **Messages** and **Files**.

Select the item you were looking for from the search results. If the results are too numerous, you can apply filters by selecting the **More filters** option.



Collaboration

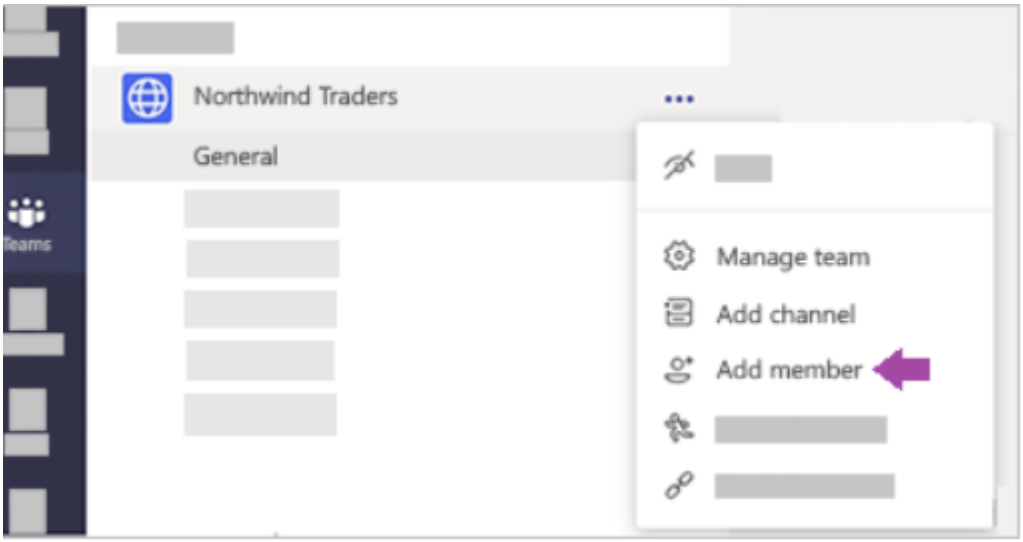
Guest Access

Allows users from outside the organization to become nearly full-fledged team members who can participate in chats and access shared files. Team owners can add guests on an individual basis. Use guest access when you want to grant an external user access to the same Teams activities, channels and shared resources as native team members.

To add a guest to your team in Teams –

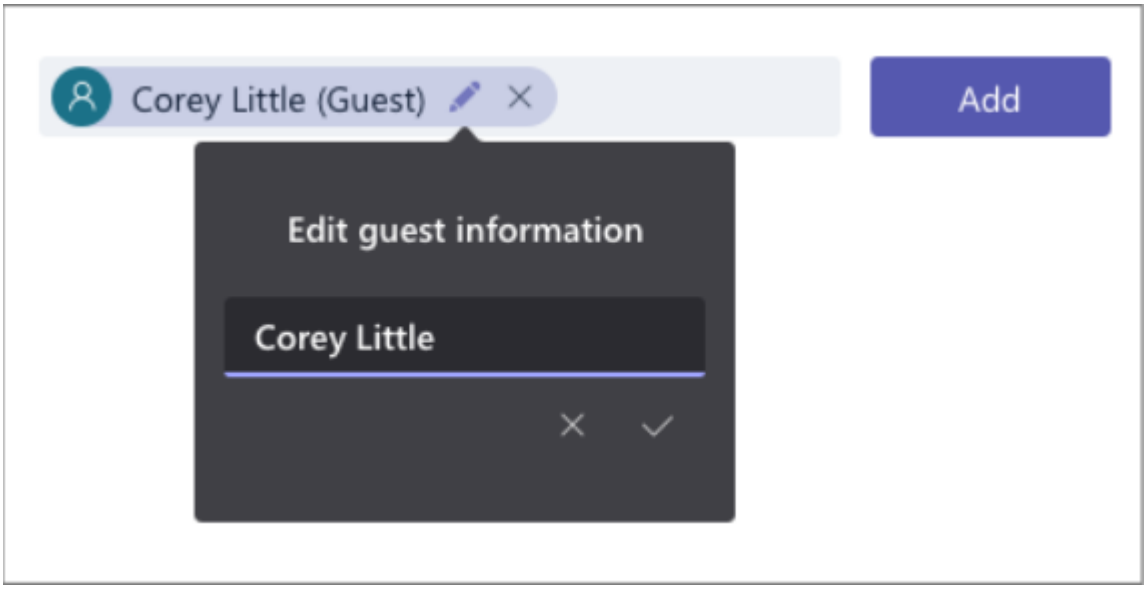
1. Select **Teams** and go to the team in your team list.

2. Select **More options** > **Add member**.



3. Enter the guest's email address. This should normally be a **business email address.** Personal email address usage should be rare provided there is no option. Anyone with a business or consumer email account, such as Outlook, Gmail, or others, can join your team as a guest.

4. Add your guest's name. Select **Edit guest information** and type their name.



11.

5. Click **Add**. Guests will receive a welcome email invitation that includes some information about joining Teams and what the guest experience is like.

Note : Only a Team Owner can add Guests to a team. Guests added to a team will be able to see all team channels except private channels (ones with padlock)

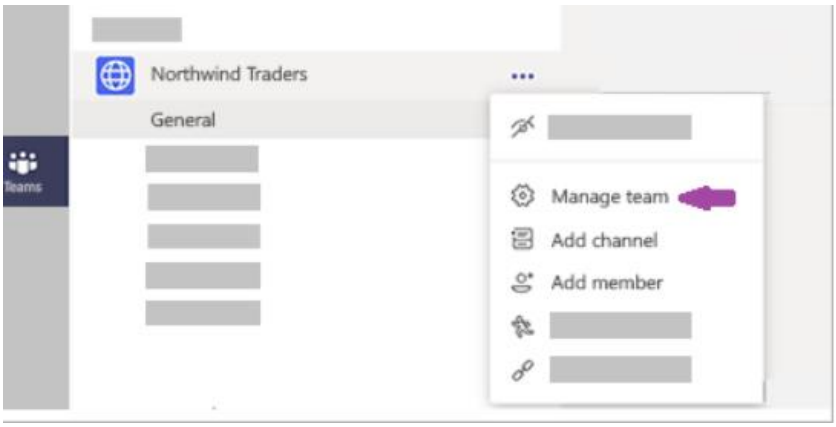
Set Guest Permissions for Channels in Teams

Guests have fewer capabilities than team members, but there's still a lot they can do in channels. Team owners can set guest permissions for channels to control this.

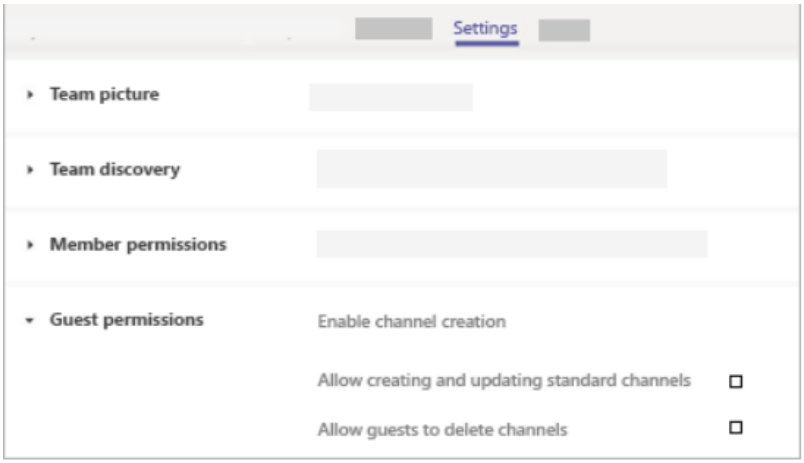
To set guest permissions for channels in Teams:

12. Select **Teams** on the left side of the app.

13. Go to the team name and select **More options** > **Manage team**.

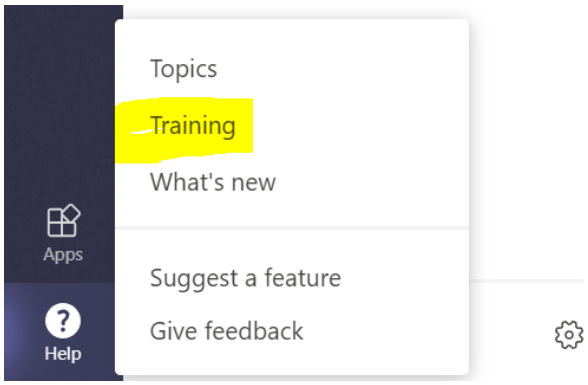


14. Select **Settings** > **Guest permissions**. Check or uncheck the permissions you want to use. Currently, you can give guests permission to create, update, or delete channels.



Discover More

If you are interested in learning more about Microsoft Teams then we would recommend clicking on “Help” in the teams app and then “Training”.



NHSCFA Service Desk

Email: ServiceDesk@nhscfa.gov.uk