

Information Governance Guidance for MS Teams

Microsoft Teams is a tool that enables users to send instant messages, make internal calls, and share, edit and collaborate on files in a central location. In addition, you can use Teams to hold meetings with anyone with an email address (local configuration dependent). This includes NHS Health and Social Care hosted and attended clinical meetings such as MDT meetings.

You must take care to ensure that you use Teams securely, and in line with good information governance (IG) and records management practice. More detailed advice and guidance can be found in your organisation's IG policies.

Teams is not intended for use with patient consultations. Please also see separate national video-conference guidance referenced below.

For patient clinical consults we would recommend the use of software intended for that purpose.

Meetings

- Guests of a recurring meeting (even if they only join once) will have full access to the chat for that meeting. You should consider setting up non-reoccurring meetings invites if guests are invited. Use the waiting room function for external guests to a meeting but be aware they will have access to chat for all meetings for that discussion. To avoid this set up a non-recurring meeting when inviting external guests.
- It is possible to record a meeting on Teams. If you intend to record meetings, please contact your IG Team in advance for support and advice to ensure you comply with data protection legislation. Additional settings will need to be set up to ensure that these recordings are only accessible from within your organisation.

Routinely recording meetings is rarely a good idea and you should explicitly state to all present what the purpose is and that it will be retained. Useful examples could be

-
- To act as an account of the meeting if a minute taker is not available
 - To share the meeting as a training tool for other colleagues
 - To allow invitees, who were not able to attend, the opportunity to bring themselves up to speed with key aspects of the meeting.
 - Be aware of what other screens you may have open when sharing screens to avoid inappropriate data being shared. Specific windows can be selected (e.g. a Word document). We recommend trying this first before doing this live on a call.
 - It is likely that you will all be making and receiving calls and video meetings when working from home or at another alternate location. Although any information which is overheard is likely to be accidental, it is important that you still respect patient confidentiality and business-sensitive data. A few simple steps you can do are:
 - Be aware of your surroundings; and in particular pay attention to what can be seen behind you. If you are working from home you should advise others present that they can be seen. You can use pre-set backgrounds within Teams to avoid this.
 - Use a headset where others can overhear you to keep discussions confidential.
 - Take calls in a separate room with the door closed; and
 - Close exterior doors or windows if open in warmer months.


Please contact your IG Team if you are considering using Teams for clinical purposes.

Creating a 'Team'

- Teams can be created for organisations by NHS Mail Local Administrators which encompass all the aspects of the Teams discussed in this document.
- A 'Team' has a designated admin user who has the responsibility of deciding which users can be added. Only users with an nhs.net or other NHS accredited email account can be added to a team – external users are automatically prohibited from joining.
- Within a 'Team', channels are created to provide a theme or heading for meetings, chats, and files to be shared. The Team admin user has the option to restrict membership to each channel e.g. if the channel contains sensitive information which should not be shared with the wider 'Team' membership.
- Team admin users can add additional admin users if required and membership to a channel or the overall 'Team' can be revoked by the admin user at any time.

-
- A number of features can be amended by the admin user in the 'Team' settings. Caution is urged when considering changing these settings as they will have been preconfigured by the Local Administrator. If in doubt, seek guidance from your local IT support team.

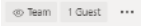
Chats

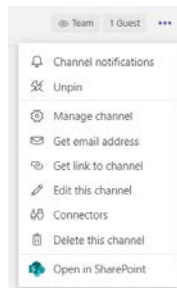
- Any message you send via a chat is retained on Teams and will be considered a record, and therefore, subject to Subject Access Requests and Freedom of Information requests. **You should not use inappropriate language or share unauthorised content. The same behavioural standards should be adhered to as if you were sending an email or speaking to someone directly.** Any record / chat / discussion pertaining to a patient record must be saved to the patient record and not stored independently on Teams. Chats on Teams can be searched by clicking on 'Chat' and entering a search term in the search bar at the top of the screen.
- Teams is a corporate system and any communication, including 1-to-1 conversations, should be restricted to corporate discussion. Personal discussion should not take place over any corporate service. Personal discussions should not take place on corporate provided systems.
- Discussions about other members of staff are retained, and these are also subject to the Data Protection Act 2018 and an individual's right of access to information held by them (Subject Access Request). This makes Teams and other email or messaging solutions undesirable for inclusion of any discussion about individuals unless it is for an agreed purpose such as an MDT. **Using Teams for personal views and comments about individuals is strongly discouraged.**
- Some Team chats are viewable by a number of users. You should always ensure what you are discussing is appropriate for the people who have access. You can check who is included in the chat by clicking the icon in the top right-hand corner . Private conversations should be undertaken in a separate Teams chat or by email.

Files

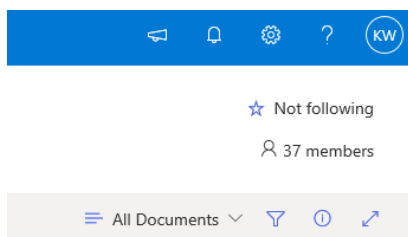
- **Teams is a collaboration workspace, and not a records management system.** With this in mind, you should continue to save important documents in the network drive locations your organisation already has in place; You may work collaboratively on draft versions of documents on Teams, or share project documents but the final version must be saved to the appropriate location on the shared drive as per normal practice. **Each discussion should appoint a role**

whose responsibility it is to save documents down to drives to avoid confusion about who is undertaking this.

- When using Teams remotely on non-NHS equipment, work files must not be synced or saved down to your own equipment. Save files to your work network locations only. If unsure please contact your local IG / IT provider.
- Although Teams is secure, data is encrypted, and it does not leave the UK, you should not, as standard practice, store or share personal data on Teams. **Teams meetings administrators (the person who organised the meeting on Teams or created a formal Team on the Teams app)** are easily able to invite additional users to a Teams page and may not be fully aware of what is being stored or shared on the page. This increases the risk of an accidental data breach occurring by a person with legitimate access to the page, inadvertently seeing personal data which was not intended for them. You can check to see who has access to a Teams page by:
- Clicking the 3 dotted icon in the top right-hand corner 
- Selecting open in SharePoint from the options



- Clicking the member's icon from the opened SharePoint webpage



Other Apps within Teams

Microsoft Teams comes bundles with many other apps. These apps have not been reviewed for good IG practice or for information security and are not therefore approved for us. Any use of additional apps is at each organisation's own risk.

More information is available at <https://support.nhs.net/>. Please contact the IG Hub or your IG team if you have any queries on this guidance, or if you require assistance with any IG matter.

Other National Guidance

The RCGP, NHSE have published guidance on video consultations. This guidance is aimed at all NHS general practice staff who are consulting via video with patients at home. It includes the key principles for safely assessing patients using a video consultation. Their guidance can be found [here](#).

NEL IG Team June 2020

Nelcsu.information-governance@nhs.net

03000 428 438