MICROSOFT TEAMS

GOOD PRACTICE TIPS

For Meeting Hosts

- Get to know and understand the way MS Teams works before your meeting
- MS Teams has the facility to create a guest list or waiting room to use if appropriate
- Be careful about advertising of meetings – think about including some distribution guidance in the appointment invite – for MDTs this could set the parameters of the organisations who are part of the MDT, and who to contact if anyone outside of that group needs to be invited on an ad hoc basis, rather than invitations being forwarded to others
- MS Teams enables the host to set screen sharing to host only should this be appropriate
- Be sure to be aware who has joined the meeting – are they all invited attendees? – no 'Zoom bombing' (where someone unexpected joins a meeting and disrupts proceedings)
- MS Teams has the facility to 'lock' a meeting once started to avoid any uninvited people joining

File and History Advice

- Manage meeting invites carefully – only include those needed
- Purge email distribution lists – for example, if you have a recurring meeting and add someone to the invite list on one occasion, that individual will be able to see all files and chat history associated with your meeting including previous ones they didn't take part in. Delete individuals from past meeting invites as needed otherwise they will still have access to future chat and information shared
- Conduct sensitive meetings separately – i.e. set up a new unique invite in Outlook, don't use recurring meeting invites
- Be cautious with sharing files – minimise access. Until we understand more about the storage of documents in MS Teams, our recommendation is not to share personal confidential information via Teams, but to use secure email transfer
- Fine to share a screen view of records or discuss confidential information within a MS Teams meeting as long as you are clear all participants should be taking part

Attendee Advice

- Manage your surroundings – ensure no sensitive information is visible through your camera view – skilled users attending could zoom in and view information
- Are others able to hear your participation in a meeting within the space you're working in? Can you wear a headset or move to somewhere a confidential meeting won't be overheard?
- Don't click on unknown meeting links – think of cyber security risks
- Be cautious with use of the 'chat' function in Teams – once you've posted something, your comment will persist (as part of our work on guidance we're working to understand what 'persist' means in this context) – so think professional, and don't post anything you wouldn't want to disclose to a wider audience. Remember, all recorded information held by a public authority is potentially subject to FOI and Subject Access rights and information within MS Teams is no different

Somerset CCG/GP DPO
July 2020