Video Conferencing & Messaging

15th April 2020 v1.0
Due to current government restrictions on travel, we need to ensure that we can continue to communicate with each other and our service users using the latest technologies.

The authority provides Microsoft Teams which should always be the preferred tool to use for Video Conferencing and Messaging whenever possible.

However, we also need to conference with our service users at times using technologies they already use, so this guidance is here to help us to do this safely.
Video Conferencing Best Practice & Etiquette

- Use Microsoft Teams as the first choice if possible
- Test your connection before the meeting begins and be punctual
- Nominate a chair/facilitator
- Use a headset to help avoid background noise, to maintain concentration and to help keep conversations private
- Mute your microphone when joining a call and when not speaking
- Introduce yourself so everyone knows who is speaking
- Be courteous, take turns to speak do not speak over others
- Be mindful of your surroundings (physical and virtual) and close any other applications prior to joining a call
Video Conferencing what do I use when?

- Video Conferencing within NCC: Microsoft Teams
- Video Conferencing with known partners: Microsoft Teams
- Video Conferencing with Service Users: Microsoft Teams, Zoom, WhatsApp
Messaging - What do I use when?

- **Messaging within NCC**
  - Microsoft Teams
  - BYOD (Teams)
  - WhatsApp

- **Messaging with known partners**
  - Microsoft Teams
  - BYOD (Teams)
  - WhatsApp

- **Messaging with Service Users**
  - Corporate Smart Phone using Text or WhatsApp
Teams - Hosting a meeting

Follow this guidance when hosting a Teams meeting:

Ensure participants attending have Microsoft Teams installed OR have tried Teams in a web browser.

Configure in 'Meeting Options' if you want people to bypass the lobby. Default is NCC staff.

Ensure 'Announce when callers join or leave' is switched on in 'Meeting Options' - Leave as Default.

Everyone can present, configure 'Meeting Options' to restrict presenters.

Teams cannot be joined in a web browser on an Apple device, use the app instead.

Be mindful not to have confidential information on display in the background.

Only share personal information verbally and only with colleagues/professionals/trusted partners.

"Meeting options" can be found in the email when booking a Teams meeting.
## Zoom - Hosting a meeting guidance

Important information when hosting a Zoom meeting, you should follow this guidance to setup the meeting to ensure control of who can join, what can and cannot be done.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meeting Passwords</td>
<td>Ensure “Meeting Passwords Enabled” is set to “On”. (Password is included in the meeting invite)</td>
</tr>
<tr>
<td>Screen Sharing</td>
<td>Set Screen sharing to “host only”</td>
</tr>
<tr>
<td>File Transfer</td>
<td>Disable “file transfer”</td>
</tr>
<tr>
<td>Join Before Host</td>
<td>Disable “Join before host”</td>
</tr>
<tr>
<td>Rejoin</td>
<td>Disable “Allow removed participants to rejoin”</td>
</tr>
</tbody>
</table>

- Under 16’s are only allowed to use the free version of Zoom
- Use a strong and 'non-work' password
- Sessions are limited to 40 minutes and 100 participants with the free version of Zoom
- Use your NCC email address, **NOT** a personal email address when signing up
- Do not share personal information or files with anyone
Zoom – Joining a meeting guidance

When using Zoom to join an externally hosted meeting you need to ensure you follow this guidance:

- **You must create a zoom account using your NCC account**

- **Ensure that if you are joining a meeting hosted by someone else, it is genuine / a trusted source**

- **Don’t allow someone else to take control of your machine**

- **Be mindful of your surroundings (physical and virtual) and do not have confidential information on display in the background**

  - Use your NCC email address, **NOT** a personal email address when signing up
  - Do not share personal information or files with anyone
  - Close all other applications prior to a meeting to prevent accidental sharing of information
What **NOT** to do!

**Do NOT:** Use your personal mobile to text service users as this will reveal your personal mobile number

**Do NOT:** Use WhatsApp on a personal device (including BYOD) to contact service users as this can reveal your personal mobile number

**Do NOT:** Ask a young person aged under 16 to install WhatsApp as it has an age restriction

**Do NOT:** Share account details or passwords

**Do NOT:** Use Facebook / Messenger to look up a service users account and contact them

**Do NOT:** Ask a young person aged under 16 to install Zoom without the consent of their parent / guardian (age restriction for children)

**Do NOT:** Capture video or audio recordings of conferences unless all participants are aware, and the content can be held securely
Due to current government restrictions on travel, we need to ensure that we can continue to communicate with each other and our service users using the latest technologies.

The authority provides Microsoft Teams which should always be the preferred tool to use for Video Conferencing and Messaging whenever possible.

However, we also need to conference with our service users at times using technologies they already use, so this guidance is here to help us to do this safely.