Using Third Party Apps for Communication during the Coronavirus (COVID-19)

Apple FaceTime, Facebook Messenger video chat, Zoom and Skype have all been approved by the NHS for business use, providing you use them responsibly.

- Consider what information you are sharing, with whom and that you can keep personal/confidential information limited.
- Determine which is the best application will meet your service requirement and customer expectations.
- Use the software recommended by your IT department with their recommended security settings.
- Only use your personal device where there is no practical alternative.
- Update security settings and enable all available encryption and privacy modes when using the applications.
- Notify users that these third-party applications potentially introduce privacy risks.
- **Do a high level Data Protection Impact Assessment. You can find a template, guidance and examples on the Veritau portal.**

Below is a bit of guidance on four of the larger and readily available options Apple FaceTime, WhatsApp, Facebook messenger and Zoom to aid you with deciding which platform will best meet your needs and some recommended settings to enhance privacy settings.

Apple FaceTime

Apple FaceTime uses end to end encryption and does not record any data during that meeting, it will however potentially collect information about who you were talking to and for what duration. It does not require a password in order to access the App, but verification of a user can be completed visually prior to starting a conversation.

WhatsApp

WhatsApp uses end to end encryption. It does not require a password in order to access the App, this could easily be accessed by an unauthorised person if they obtain

Veritau
Assurance Services for the Public Sector

your device. Your device is the security concern as this is where conversation history is held and information could be breached if put into the wrong hands. If you back up your WhatsApp messages on your device these backups are decrypted messages, and you are reliant on the back up services cloud settings to keep your data secure.

If work WhatsApp groups are created there is a risk that if used for official messaging, they will still have access to that data even after they leave, or they are not removed from the group on departure and receive new information.

WhatsApp has access to your address book and other contacts, and updates from them on a regular basis, this includes any of your contacts that have not subscribed to WhatsApp. It can piece a picture together quickly if you have social services number in your phone and an addiction clinic for example. It also collects further data like tracking information, device data (down to your battery level, network, IP address and signal strength) and cookie information.

WhatsApp is part of the “Facebook Family”, meaning data is shared between the SMS app and its parent company. The information gleaned from WhatsApp isn’t publicly available, instead being added to Facebook’s hidden profile of you. It remains one of WhatsApp’s biggest security concerns. Facebook have widely known security concerns over how they handle, protect and share personal information.

WhatsApp is used by businesses that can access your contact details for marketing as well, and Cybercriminals will use this method to launch Malware and phishing attacks such as:

- GIF attack where an image is sent to a user on WhatsApp that enables a hacker to see all your conversation history.
- Pegasus voice call hack. This is where a hacker puts a WhatsApp voice call to its target and installs malware, this can be effective even if the call is not answered.
- FakeApp attack where a hacker can plant fake responses in group chats that appear to be from legitimate users and change the text of replies.

There is also no way of controlling any data you have shared with recipients, once received it is easy for them to make that information publicly available by posting it on various media platforms including Facebook.

Update your Privacy Settings on WhatsApp

Ensure your WhatsApp version is always updated to receive any security patches.

Enable Touch ID to open WhatsApp, under Account, Settings, Privacy, Screen Lock.

Through your Account privacy settings on WhatsApp, you can control who can see each of three pieces of information about you: your profile picture, your personal status message, and when you last used the app (if you're offline). If you choose "Everyone," all users can see that piece of information. If you choose "My Contacts," only people whom you have added as contacts can see that information. Choosing "Nobody" prevents anyone from seeing that information, whether they are your contacts or not. Note, however, that you cannot choose to appear offline if you are currently online with WhatsApp.

WhatsApp has a function called "read receipts" that sends you a notification when someone reads a message that you sent them and vice-versa. You can turn this on or off as you choose, though it only applies to personal conversations and not group chats.

Ensure you disable live location, and check your smartphone permissions to ensure you have not granted it to other apps unless it's really needed.

Delete any old message threads you no longer need under Settings, storage usage.

Facebook Messenger

Facebook Messenger uses secure end to end encryption but only through the use of the Secret Conversation option. You can't have a Messenger account though without first having a Facebook account.

Facebook have large security concerns over Facebook was hit with a record $5 billion fine from the Federal Trade Commission in July 2019, and £500,000 fine from the ICO over issues like the Cambridge Analytica data scandal, using phone numbers intended for two-factor authentication for advertising and accidentally storing passwords in plaintext. Facebook also conducts web tracking on users even the app is not in use, they also use algorithms to aid targeted marketing use. They meticulously scrutinizes the details of its users' online lives, its tracking stretches far beyond the company's well-known targeted advertisements.

Making Facebook Messenger more secure

Enable Secret conversations by opening the Facebook Messenger pp and clicking on your profile picture top left. Select 'Secret Conversations' and ensure you turn it on.

If you have your contacts synced on your Facebook Messenger app, Facebook might have access to your call and text message history. To turn this off, go to messenger and click on your profile picture on the top left. Then click 'People' in the menu, and turn of Upload Contacts**.**

Review your Facebook Security settings though Facebook Settings, Security and login.

Enable two factor authentication, to stop your account being accessed from an unrecognised device.

Review devices that are authorised to login to your account.
Turn on get alerts for unauthorised logins.

Zoom

The Ministry of Defence have dropped the use of Zoom due to security concerns, and the increase in demand due to COVID-19 has vastly exceeded their regular usage. This has raised concerns over if the company has the staff and capability to cope with the demand without detriment to the service whilst maintaining and updating security. Zoom have known about a security flaw where Hackers can easily join your meetings via brute force since 22 July 2019 and claimed they had addressed the issue in August 2019.

Samurai Digital Security Ltd exposed the same flaw on the 26 March 2020; they completed a 30-minute scrum hack and found and joined meetings via brute force. They can take over a presenter's audio and pretend to be them or just listen into the conversation. This is despite passwords being set. This is all done by obtaining your meeting ID which is easy to obtain via a browser. If dial in is available, then ensure you look out for 'Call-In User_1' or any number above the expected participants and confirm their identity.

Making Zoom more secure

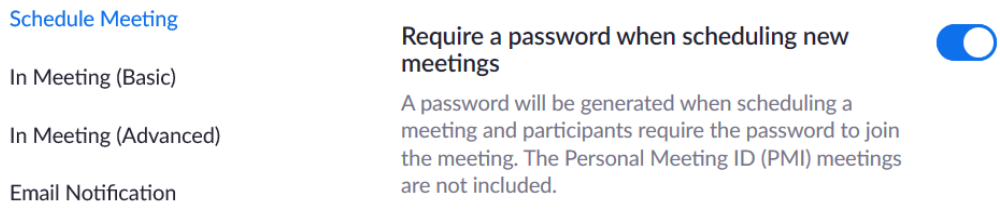
If you do decide to **accept the risk** and use Zoom then **don't rely on Zoom's default settings**. You must apply additional security layers and the following guidance will assist you in remaining as secure as possible:

Harden your system against attack using Zooms security configuration:

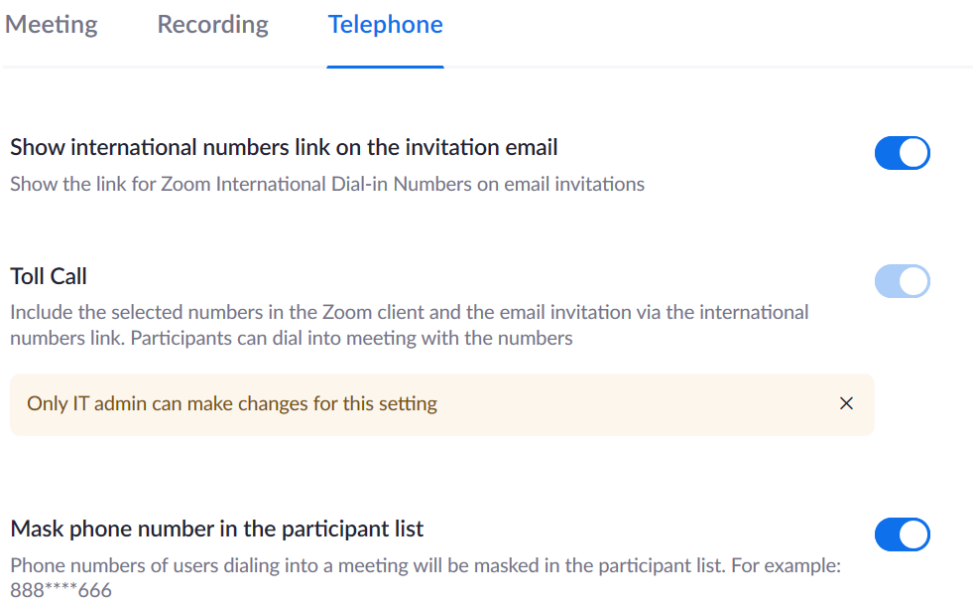
Choose carefully who holds the Admin account, ensure they have a strong password in line with your policy and they apply adequate security settings.

There are lots of extra security settings that can be utilised to enhance security. As a minimum users should consider applying the following security settings to protect their meetings using: https://zoom.us/account/setting/. These must be applied **before** a meeting:

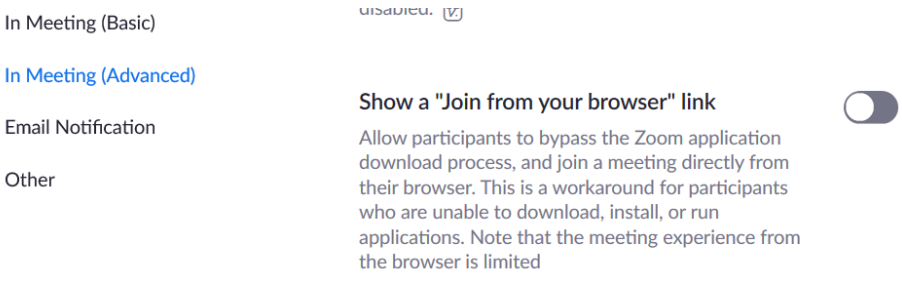
1. Enforce the Pin code/password for anyone joining by phone via Zoom account settings in the administrative panel. This must be turned on before you initiate the call under the schedule meeting heading.



2. If someone dials in using the prefix 141 this masks their number. You have an option under account settings to Mask phone numbers in the participant list and this will apply to all and prevent disclosure of their number. Use the Telephone tab at the top



3. Enable the Join from Browser link under the Meeting Tab, In Meeting (advanced). This will allow users to join via a browser using a onetime generated code. This is a secure way of joining as long as you enable Two Factor Authentication as well see point 4 below.



Veritau
Assurance Services for the Public Sector

4. Ensure that only authorised users can join the meeting using two factor authentications. Two-factor authentication (2FA) is a two-step sign-in process that requires a onetime generated code on a mobile app in addition to a Zoom username and password. Users will need to download the authenticator app first this provides an additional layer of security since users will need access to their phone to sign in. The following apps can be used:

    - Microsoft Authenticator (Android, iOS, Windows)
    - Google Authenticator (Android, iOS)

    Only the Admin can enable 2FA and setup a 2FA user. Further guidance on how to enable, set up and sign in using this service can be found at https://support.zoom.us/hc/en-us/articles/360038247071

5. Ensure you password protect the meeting on setup (this still can be worked around) and if you are not expecting anyone to dial in then disable the telephone option under Audio by selecting Computer Audio.