Things to think about when video-conferencing

Dear Surrey resident
This will be 10th and the last Alert of the set regarding protecting yourselves on line.
More Alerts/emails will follow as and when needed.
This one is on the things you need to think about when video-conferencing via Zoom, Teams, Houseparty, etc. Most of these provide a basic free service although often with a time limit.

The COVID-19 lockdown means many of us are now using video calls to stay in touch with family, friends and work colleagues. Even when lockdown lifts, video meetings will still be with as they are often more convenient in many cases. If you're new to video conferencing, this guidance will help you to use these services safely.

Even if you're familiar with video conferencing, we recommend you take a moment to check how you're using it to ensure you do so securely.

What is video conferencing?
Video conferencing is a live audio and video conversation between 2 or more people in different locations, conducted using phone, tablet, laptop or desktop computer. Most video conferencing services also allow you to view another person's screen and so share pictures and information.

Regardless of whose service you use, this guidance is applicable to all video conferencing services.

Downloading video conferencing software
If you're downloading standalone video conferencing software, make sure that you:

- Only download the software from trusted sources. This means using your phone or tablet's app store (such as Apple's App Store or Google Play), or downloading the software from the service provider's official website.
- Check online to understand what app is right for you. In most cases, the 'free' version of a video conferencing service will provide good enough functionality and security for personal use, provided you've set it up correctly.
- Check the privacy settings. You should make sure that you understand what (if any) data the service will access during operation. You may have the option to opt out of sharing data.

Setting up video conferencing services
Before making your first call, you should:

- Make sure your video conferencing account (or the device or app you are using for video conferencing) is protected with a strong password. If you need to install the video conferencing app, you'll have to create an account for it.
- Test the service before making (or joining) your first call. Most services have a 'test' function to ensure your microphone and camera work correctly, and that your internet connection is fast enough. You can also use the test function to learn how the service works. As a minimum, make sure you know how to mute your microphone and turn off the camera. This

will give you more control over what you share with others. If still nervous ask the organiser to have a test meeting with you before the main meeting.

- Understand what features are available. Many services allow you to record the call, share files, or show what is on somebody's screen. Find out how to tell if the call is being recorded, what exactly is recorded (audio, pictures, messages), and who can access the recordings. There may also be additional controls to manage who can join the call.

Hosting and joining calls

It's important that you can control who can join your video conferencing call. For specific instructions, refer to the support website of the service you're using. However, the following general rules apply:

- Do not make the calls public. Connect directly to the people you want to call using your contacts/address book, or provide private links to the individual contacts. For some video conferencing services, you can set up the call so that a password or code is required in order to join. This adds another layer of protection. Do not post the link (or the password/code) publicly.
- Know who is joining your call. If you are organising the call for your family or friends consider using the lobby feature to ensure you know who has arrived. This is especially useful if individuals are joining the call via an unrecognised phone number. Make sure people are who they say they are before they join the call (the password function described above can help with this).
- Consider your surroundings. Take a moment to think about what your camera shows when you're on a call. Would you want to share that information with strangers? Consider having a screen behind you blocking off the view.

Finally, make sure that all your devices and applications (not just the video conferencing software) are kept up to date. Applying software updates is one of the most important things you can do to protect yourself online. Update all the apps (and your device's operating system) whenever you're prompted. It will add new features and immediately improve your security.