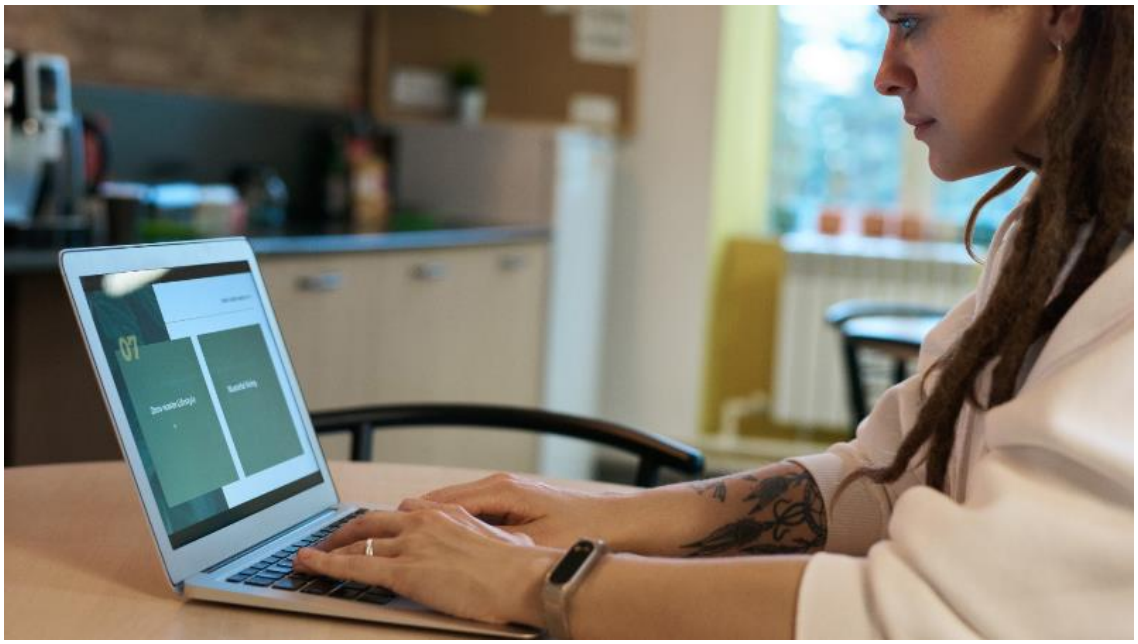
Remote working options and tips



We should all by now be planning for remote staff working whether this be due to self isolation or potential full office closure. We have put together some practical guidance for how tech can help, including best practice to minimise any security risks.

The ideal solution would be for staff to use work laptops and other devices. If this is not possible (we appreciate this is unlikely to be the case in many small, local charities), there are some protocols you could introduce to minimise risk.

1) If staff or volunteers need to use a shared PC (with other members of their family or flatmates):

- Where possible, do not download documents containing confidential or personal data (information that identifies individuals)
- If this is unavoidable, ensure that you delete files from local drives and also from your recycle bin after use

- If using Office 365 or other online access to files and email, or online databases / CRM systems, always log out of your account and close your browser after use. Then re-sign in each time you need to access it (avoid ticking – remember password or stay signed in options)
- Where possible – set up a different Windows or Mac user account for work use, to minimise others in the household accessing organisational data if saved locally unintentionally

2) For those of you using Office 365, this gives a great range of tools that will be useful for working remotely, allowing us to communicate and collaborate. Teams offers the following:

- A Chat facility where you can converse within your Team and take communications off email as appropriate
- Conversations and Commenting on documents you need to collaborate on
- Voice calls - a useful way to make individual or group calls across the team or hold online meetings internally which can be recorded. Purchasing headsets with microphones would be a good idea if you are likely to use this feature regularly (these seem to be in great demand and Amazon and Argos were restricting purchases to one of each model at the weekend).
- Adding external users - please contact us if you need to us to 'switch on' inviting external users into your Team space. This works well if you need to collaborate with external partners or for example Trustees or Volunteers who don't have an organisational email address
- Adding Channels within a Team. This can help separate different workstreams and now you can select whether a Channel can be accessed by all members of your Team, or choose for it to be Private, and only accessible to Team members you select

- Downloading the Teams app to desktop or mobile device and enabling alerts so you can see for example when someone has @mentioned you in a conversation

If you are not familiar with these features we recommend you try these out in the office over the coming days. There are some great learning videos here to share with staff and learn more about how Teams can help. You can also download the Crash Course in Microsoft Teams as a pdf for a comprehensive overview.

3) Please also remind all staff about general IT security and best practice to follow. Useful resources and advice to share include:

- Superhighways' blog posts on a range of IT security considerations including our Phishing email awareness raising video The National Cyber Security Centre have posted a blog highlighting that there have been a number of phishing attacks exploiting worries over the Coronavirus
- National Cyber Security Centre - Cyber Security training for staff
- Think about how secure your wifi is. It is safer to hot-spot to your phone for internet access than to use insecure shared or free wifi