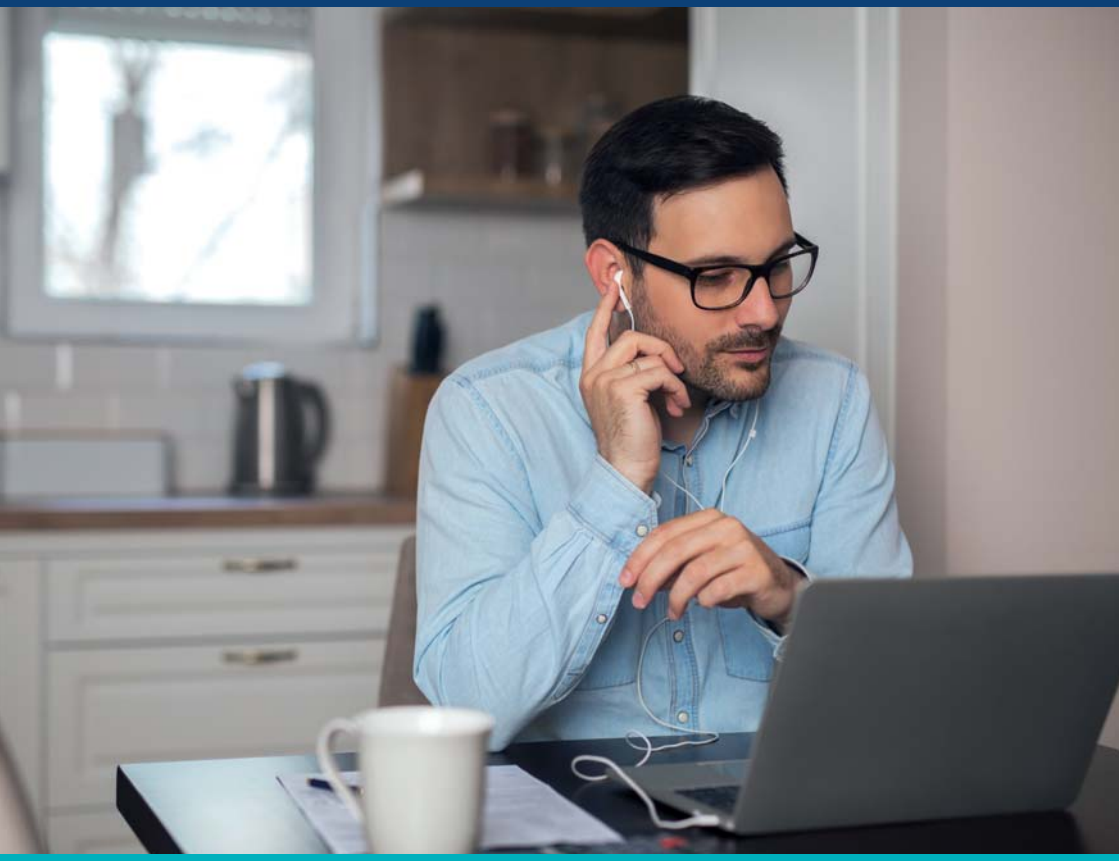
ROYAL AIR FORCE

Working from home



Keep it safe and secure

GET SAFE ONLINE .org

www.getsafeonline.org

Advice for working from home or other remote locations.

Depending on your unit, role and individual circumstances, you may already be familiar with home working and what you need to do to help keep yourself and the RAF protected online.

Whether this is the case – or it's a new experience – it's important to remind ourselves that **as a workplace, the home is very different from our normal work location**. This is partially owing to technical restraints such as devices and internet access, but also the other aspects of our lives that are always present, such as our children and, currently, our concerns for our own and loved ones' continuing health, welfare and wellbeing. And the fact that we also tend to be more relaxed in our own homes, and therefore potentially less guarded about potential online threats. Our adversaries are fully aware of these vulnerabilities and have increased their activity accordingly, including via social engineering and attempting to extract sensitive information through installing malicious software.

Please regard this leaflet as a guide to good practice or a reminder, make sure you follow the advice and suggest to colleagues that they do the same.

ROYAL AIR FORCE

- **Protect MOD devices and information** in a suitably secure and / or concealed location at home or whilst commuting or travelling.
- Make sure your **Wi-Fi connection is set to secure**, protected with a strong password and not readily recognisable as yours from its SSID (Wi-Fi network name).
- **Never use public Wi-Fi for RAF work** in case it is either not secured, or a fake router impersonating that of the premises where it's located.
- **Make sure work information can't be seen by others** at home. Check that you're not overlooked, and if you have to leave your device then either lock the screen (Ctrl, Alt, Del on Windows devices) for short periods or turn it off for longer ones.
- When making work calls or having work conversations, do so **out of earshot of smart speakers** (for example Amazon Echo or Google Home) or cameras, or disconnect them before the conversation.
- Make sure you're using **MOD-approved headphones and cameras** if using them with Skype.
- **Lock away or conceal sensitive documents** when not in use, or you step away from them for any length of time.
- If you do have to leave home with ICT or documents, **don't leave them unattended** in a vehicle or train, in a cafe or other location.
- **Don't let it be known that you are an MOD employee and working from home**, either on social media, other online platforms or casual face-to-face conversations.
- **Never under-classify information**, including for the purposes of working on it from a MoDNet laptop. Doing so represents a serious security breach. Also, **never create or process SECRET or above information** whilst working from home.
- **Don't re-direct MOD email** to a personal email account, and do not use your personal email account to routinely share documents or conduct MOD business.
- **Don't use MOD devices to browse the internet for non-work-related content**. Doing so represents a security risk.
- **Work documents must not be printed** at home or other locations other than MOD premises. Personal printers and other devices must not be connected to MOD devices.
- The walls have ears! **Don't hold sensitive phone conversations in public**.
- **Don't dispose of printed work information in your household waste**. Instead, return it to an MOD office or duty station when you can return there.
- **Report any loss or compromise** of your device or hardcopy information **immediately** to your Line Manager, WARP or Local Security Officer.
- If for any reason you become too ill to work, **ensure MOD devices and information have been secured**.

Working from home for the first time

- Ensure the laptop has been **physically connected** to the network in order to pick up the latest software updates, including antivirus and security patches.
- Check that the **remote connection** is working normally.
- **Update your MoDNet password** so that you will be able to continue to work remotely, as you need to be connected to the LAN for system-mandated password changes.
- Note that all laptops must be regularly **physically connected to the MoDNet network (in the office)** for at least two hours to download software updates.

As you would in your normal workplace, report any email you believe to be suspicious by doing the following:

1. Create a NEW email (do NOT use the Forward button).
2. Drag and drop the suspect email from your inbox into the body of the new email, embedding it as an attachment.
3. Copy the subject line from the suspect email into your new email exactly as it appears.
4. In your new email, indicate whether you have or have not clicked on any of the links, buttons or attachments in the suspect email.
5. Send the new email to SPOC-SPAM@mod.gov.uk
6. Delete the email using [Shift]+[Delete] to wipe the email from your inbox. Make sure you delete both the original and your 'Sent' email, and remove them both from your Deleted Items.

For comprehensive, practical, expert advice on keeping safe and secure online, visit **www.getsafeonline.org**
#RAFsafeonline

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by a number of government departments, law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

GET SAFE ONLINE .org

ROYAL AIR FORCE

www.getsafeonline.org

GET SAFE ONLINE: WORKING TOGETHER WITH...

TESCO · NatWest · Gumtree · Standard Life · first direct · HSBC · ROYAL AIR FORCE · Royal Bank of Scotland · M&S BANK · LLOYDS BANK · HALIFAX · BANK OF SCOTLAND · creativevirtual

CITY OF LONDON POLICE · NPCC · NATIONAL TRADING STANDARDS eCrime Team · cifas · VS VICTIM SUPPORT · EUROPOL EC3 European Cybercrime Centre

ActionFraud · METROPOLITAN POLICE · Ofcom · neighbourhood ALERT