Security considerations for remote working

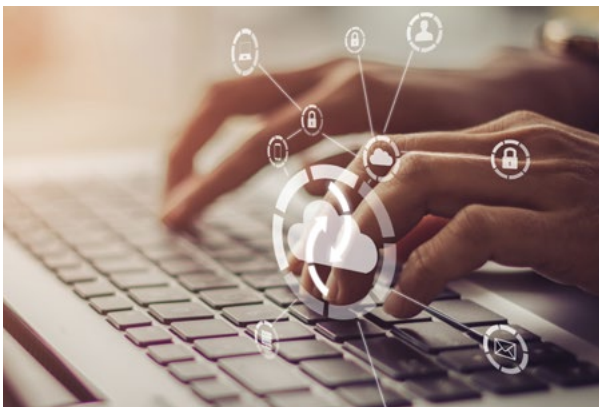
As colleagues and volunteers will potentially access information and communicate using their own devices, please consider the following:

Increased risk of computer viruses and vulnerabilities

- Keep anti-virus software up to date
- Don't re-use or share passwords
- If working in public, such as in a café or on a train, avoid inputting passwords or sensitive information.
- Avoid using public Wi-Fi if possible.

Storing and sharing files

- Sensitive information such as identity checks or performance reviews should not be stored locally on your personal device.
- Create a secure, central location on a tool such as Microsoft OneDrive or in your organisation's shared space.
- Provide training on using any storage or file sharing tools.



Phishing and spam

- Spam or junk email is not just a nuisance; it may also aim to encourage the recipient to click on links or reveal personal information.
- This represents a form of deception called ‘phishing’ whereby someone may attempt to trick the recipient into believing fake and deceptive information with the hope they might reveal bank or credit card details or passwords
- Ensure your remote workers are aware of these kinds of pitfalls so as not to compromise the security and safety of your organisation’s details as well as their own.