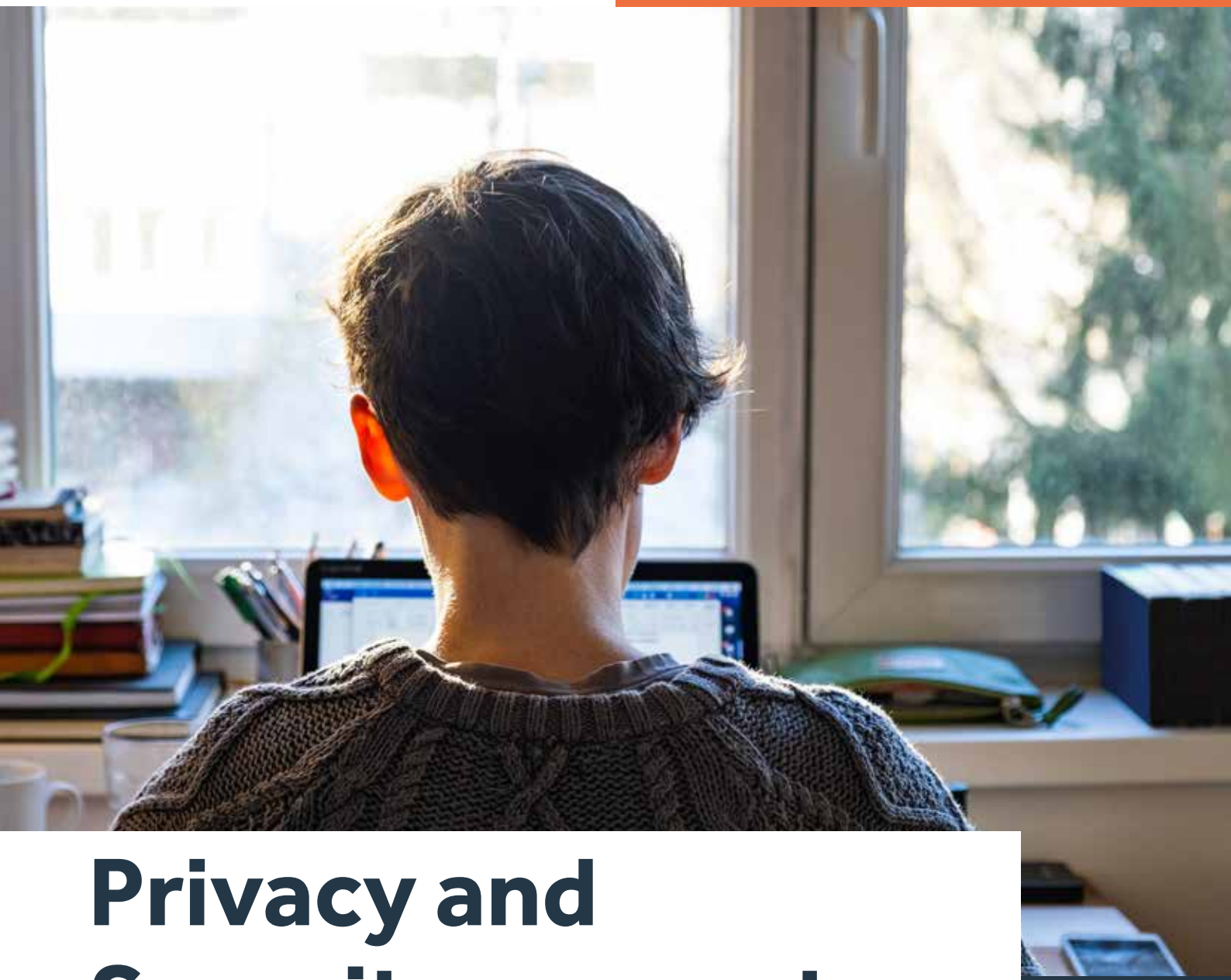
EduCare® Part of tes



Privacy and Security support

when remote working for the first time

As the coronavirus pandemic has forced many of us to work remotely, some of us for the first time, it is important that these adjustments to the ways in which we work are done with security and data privacy in mind.

In this resource, we will provide good practice guidance for when working remotely and making sure you are equipped to do your job whilst staying alert to the cyber security threats and your data protection obligations.

Remote Working good practice

Even in this challenging time, the obligations in the General Data Protection Regulation (GDPR) must be carefully considered and upheld. Some simple steps you should consider include:

- Using a work issued device, email and other logins where possible.
- Keeping your device(s) updated to the latest operating system.
- Making sure your device(s) are password protected and locked when not in use.
- Storing your device(s) securely when they are not being used.
- Minimise the storage of personal data on your device(s).
- Storing personal data in secured, access controlled locations.
- Ensuring your device(s) are encrypted if processing personal or other sensitive data.
- Making sure data is backed up regularly.

Have you got all the tools you need?

Staff who are used to being in the office may not have all the tools they need to be able to operate fully now they are working remotely. You should consider whether there are new tools you may need to operate effectively outside the office.

If you are not equipped to do your job, you may find different ways of working which are less secure so you should let your IT and Security teams know what you need.

If you are thinking of using new tools, you should consider:

- Make sure you are only using software approved by the organisation you work for, if you do not have the right tools, ask for them.
- Set up any new tools by following the instructions carefully and, where available, set the tools up with security like Two Factor Authentication (2FA).
- Ask for guides, training or online resources to learn the best ways to use the tool.
- Make sure you are familiar with how to report any problems with the tool.

Where applicable, you should have up to date antivirus installed on any devices you are using to access the internet.

Extra vigilance to social engineering tactics

Social Engineering is the broad term for the tactics used by cyber criminals to gain access to data and/ or your credentials.

They use deception, urgency and manipulation to get login details and/ or infect your device. Common variances of these include phishing, spear phishing and vishing attacks.

You should be extra vigilant when working remotely, especially as cyber criminals look to exploit people's fears about the Coronavirus pandemic. Here are some tips to help you spot phishing emails:

- Look out for bad grammar, punctuation and spelling.
- Is the email addressed to you directly or something generic like 'colleague' or 'friend'?
- Does the email impose an unnecessary amount of urgency to respond or 'sign in'?
- Look at the sender's email address or name, does the email address match those you are familiar with or are there subtle differences?

A real sender will not have issue with you contacting them directly to check the email is genuine. If you do receive a phishing email, you should contact your IT team.

If you have clicked a link, don't panic. If you are on a work device, contact your IT team.

If you are using a personal device, and feel comfortable doing so, run a full scan and follow the instructions. In any case you should disconnect from the internet immediately.

If you have provided passwords and usernames, go ahead and change them as soon as possible.

The National Cyber Security Centre

Provides a guide on spotting and responding to phishing emails.

Perfect Passwords

More so now than ever, the passwords that you rely upon to secure access to vital tools and data should be robust.

A good password is a free, easy and effective way of preventing unauthorised access. Here is what you need for a strong password:

- A great way of creating passwords is by using a string of random words.
- They should be complex but memorable.
- You should avoid using personal information like your pet's name, your place of birth or your child's name as well as easily guessable strings such as '123456' or 'password'.
- The longer a password is, the better it will be. You should avoid using very short passwords. You should follow your company's protocols on minimum length and special characters when setting passwords.

To keep your password secure:

- Use different passwords for each account and service you use.
- Consider using a password manager for the storage of all your passwords.
- Use Two Factor Authentication (2FA) where it is available
- Always lock your device and log out of accounts when they are not in use.

Data Protection and Coronavirus

The ICO have recognised the unprecedented challenges faced by organisations during the Coronavirus pandemic. Data Protection will not stop organisations from adapting the ways in which they work, any changes that you make to the services your organisation offers you must be done in reasonable ways that your customers would expect.

Ultimately, the GDPR and Data Protection Act 2018 are laws, so statutory time frames for breach reporting and responding to data subject requests should still be met while you are working remotely. You may need to look at the ways in which you and your organisation report data breaches internally to ensure these functions are fit for purpose in a remote working world.

Coronavirus and the Information Commissioners Office

Read more advice about Coronavirus and the ICO's approach to enforcement on their **website.**

The Basics of Cyber Security when working remotely during the COVID-19 Outbreak

There are simple but effective steps that you can work into your daily and weekly routines to keep you, and your organisation safe whilst working remotely.

- If you need new accounts to work remotely you should set strong passwords for user accounts. You should, where possible, set up two-factor authentication (2FA).
- Where you use passwords, you should always use unique passwords, they should be stored in secure password management software, they should be complex but memorable and, ideally, only changed when you suspect they may have been compromised.
- Devices used when working remotely are more vulnerable to theft and loss. They should be stored securely when not in use. You should familiarise yourself with your organisations process for reporting this to the IT team. The earlier you can report this, the easier it will be to respond effectively minimise and data loss.
- The use of removable media, such as a USB or external hard drive, carries a significant risk. When you are working remotely, you should limit the amount of data, particularly sensitive and personal data that you are storing on such devices and they should be adequately protected with encryption. There are more secure technologies now available for the movement of data. Your organisation might have even disabled USB ports to prevent the use of removable media.
- Where possible you should utilise the collaboration tools your organisation already has to share information, if you need something to work effectively follow your organisations procedures to request it.
- Stay vigilant to social engineering and familiarise yourself with the previous tips on how to spot a phishing email.

Further information

ICO

NCSC

NCSC
Password guidance

ENISA
Tips for cybersecurity when working from home

World Health Organisation Coronavirus Criminals

The WHO have provided a brief on criminals disguising themselves as WHO officials trying to steal money or sensitive information. Read more advice about Coronavirus WHO's updates on Cyber Scams.

EduCare® Part of tes

Web links =