National Cyber Security Centre

Cyber security
For 'Early Years' education and childcare practitioners

Early Years education and childcare settings, like most other work environments, are increasingly reliant on technology. The steps below can help practitioners working in Early Years settings to protect the data and devices they use every day.

Why does cyber security matter for Early Years practitioners?

Cyber security is about protecting the devices we use every day, and the data that all businesses - large and small - need to function.

For Early Years practitioners, cyber security can help safeguard the children in your care. It can help protect the personal or sensitive information you hold on children and their families.

Even small settings hold information that is of value to a criminal. And although they may not target you directly, it's all too easy to be damaged by scam emails that cyber criminals send out, indiscriminately, to millions of businesses.

Even if you think you're not at risk, we'd encourage you to follow the four steps on this page. Doing so will reduce the likelihood of you being a victim, and help you get back on your feet should the worst happen.

1. Back up your important data

Keep a backup copy of your essential information in case something happens to your IT equipment, or your setting's premises:

- Make a list of the most important information (that is, the information that your setting couldn't function without), or information that you're legally obliged to safeguard.
- Copy this information onto a USB stick or an external hard drive or 'in the cloud'. Make sure you that know how to recover the information from it. If you're not sure how to do this, search online for instructions.

2. Use passwords to control access

You can use passwords to prevent anyone who's not authorised from accessing your email, your devices, and the data you store on them:

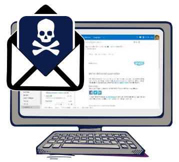
- Make sure that your laptops, PCs and tablets require a password, fingerprint, PIN or screen-pattern when first switched on (and 'lock' them when they're not in use).
- Avoid using predictable passwords (such as dates, or family/pet names) or the most common ones (like 'passw0rd').
- Don't use the same password across different accounts. In particular, use a strong and separate password for your email.
- To help you remember passwords, save them in your browser, or write them down and keep them safe (away from your computer).
- Check the privacy settings when posting photos (or other details) on social media, so that only carers have access. You should also consider adding password protection to any newsletters you send out.

3. Protect your devices

Your devices can become infected from an email attachment that contains a virus, or by plugging in an infected USB stick, or even by visiting a dodgy website:

- Keep your antivirus product (included with most computers and laptops) turned on and up to date. Most modern smartphones and tablets don't need antivirus software.
- Don't put off applying software updates - they include protection from viruses and other security updates. Update all apps and your device's operating system when you're prompted.
- Turn on 'automatic updates' in your device's settings, and in your antivirus software.

4. Dealing with phishing emails



'Phishing' emails are scam messages that try to convince you to click on links to dodgy websites, or to download dangerous attachments:

- Spotting scam emails is tricky, but look out for official-sounding messages, emails full of 'tech speak' (designed to sound more convincing), or emails that urge you to act immediately.
- Remember, your bank (or any other official organisation) will never ask you to send your password by email. If you have any doubts, contact them using their official website or social media channels.
- If you receive a message that doesn't feel right, report it to the NCSC's Suspicious Email Reporting Service (SERS) at report@phishing.gov.uk .

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq