Early Years practitioners: using cyber security to protect your settings

How to protect sensitive information about your setting and the children in your care from accidental damage and online criminals.

Early Years education and childcare settings[1], like most other work environments, are increasingly reliant on technology.

Smartphones, computers, laptops and tablets are a fundamental part of modern life. From online banking and shopping, to email and social media, to the 'smart' devices that monitor and protect our homes and work premises - it's difficult to imagine how we'd function without them.

That's why it's more important than ever to take steps to protect these devices (and the data we store on them) from accidental damage, or from online criminals. And it's also why **cyber security** is important to **all** of us. Cyber security is about safeguarding the devices we rely on, and protecting the services that all businesses, large and small, need to function.

Why does cyber security matter for Early Years practitioners?

For Early Years practitioners, cyber security also plays a role in safeguarding the children in your care. Good cyber security means protecting the personal or sensitive information you hold on these children and their families. Your national Early Years legislation and advice[2] and the Data Protection Act require you to hold confidential information and records about staff and children securely, and ensure these can only be accessed by those who have a right or professional need to see them (either physically or digitally/online).

You may not think it, but regardless of the size and nature of your setting, **the information that you hold is of value to a criminal**. And although they may not target your setting directly, it's all too easy to be damaged by scam emails that cyber criminals send out indiscriminately to millions of businesses.

Cyber criminals will go after anybody, provided there's money to be made. Even if you don't lose money directly, a data breach (which is when information held by

a business is stolen or accessed without authorisation) could cause temporary shutdown of your setting and reputational damage with the families you engage with. It could also leave you open to an investigation by the Information Commissioner's Office (ICO).

This may all sound quite alarming, but there's no need to panic. This guidance from the NCSC has been produced to help practitioners working in Early Years settings to protect the data and devices you probably use every day. It could save time, money and even your setting's reputation.

Even if you think you're not at risk, we'd encourage you to read the guidance. Following the four steps outlined below will reduce the likelihood of you being a victim, and will help you get back on your feet should the worst happen.

---

1. Back up your important information

Think about how much you rely on technology to run your setting, and the information stored on your computers. This includes sensitive information about the children in your care, their families, staff records, family contact details in an emergency, and other highly personal information. There's also business-critical data such as email, fee payments, banking and invoices.

Now imagine how long you would be able to operate without them.

It's important to keep a backup copy of this essential information in case something happens to your IT equipment, or your setting's premises. There could be an accident (such as fire, flood, or loss), you could have equipment stolen, or a

computer virus could damage, delete, or lock your data until a ransom is paid. The NCSC has produced advice to help respond and recover from ransomware attacks.

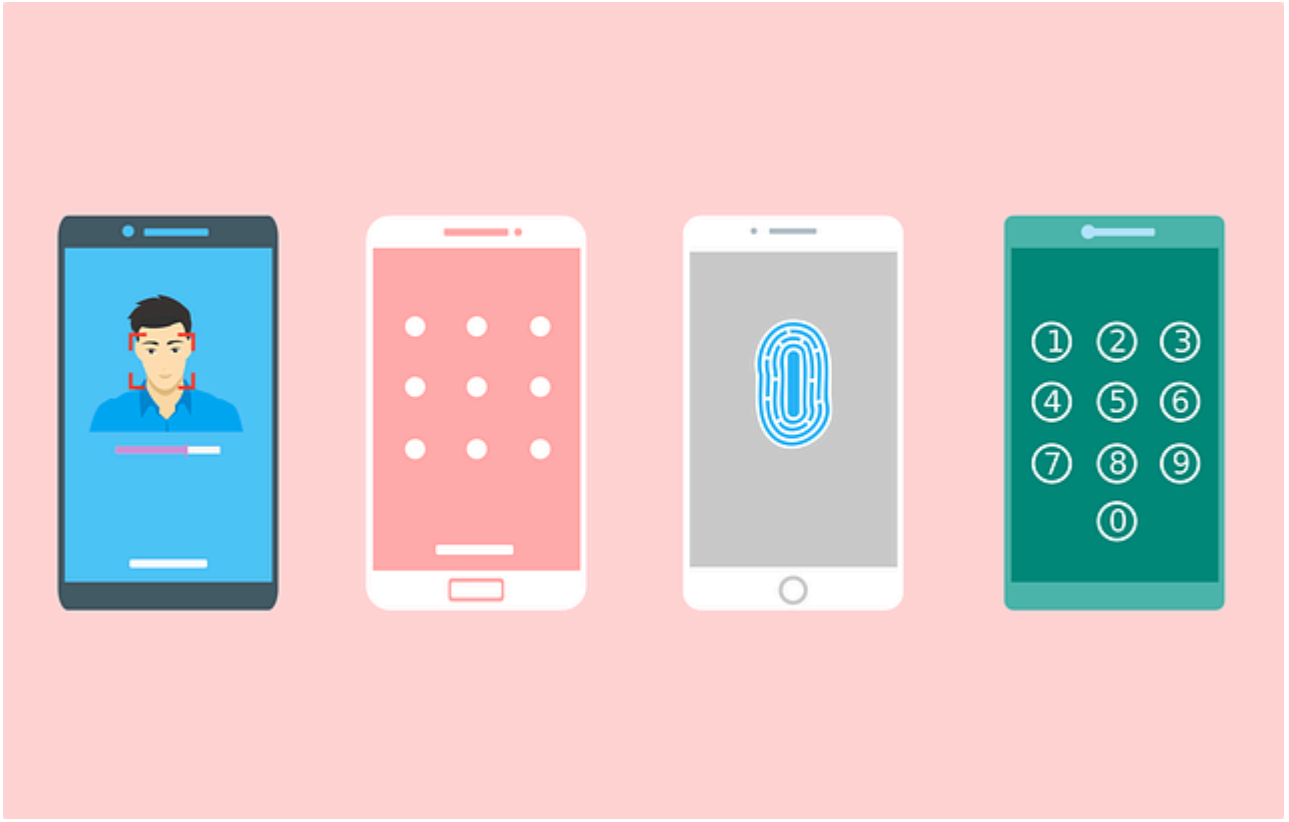
Start by identifying your most important information - that is, the information that your setting couldn't function without or that you're legally obliged to safeguard. Make a backup copy on a USB stick, an external hard drive, or 'in the cloud'. Having made your backup, make sure you know how to recover the information from it. If you use nursery management software, it will probably include tools to help you do this. If you don't use nursery management software, search online for instructions. To get you started, here are some 'how-to' guides for setting up cloud storage:

- Apple (iPhone, iPad and iPod Touch, and Mac)
- Google (Android)
- Microsoft (Windows 10) devices.

---

2. Using passwords to control access to your computers and information

When used correctly, passwords are an effective way to prevent anyone who's not authorised from accessing your email accounts, your devices, and the data you store on them. This section outlines some things to keep in mind when using passwords.



Switch on password protection (or other 'sign-in' options)

Make sure that the devices in your setting (so laptops, PCs and tablets) require a password when you switch them on. If you'd rather not use a password, choose another method to 'lock' your device, such as a fingerprint, PIN, screen-pattern or face recognition. If you need help doing this, we've included some links below:

- Sign-in options for Windows 10
- Sign-in options for Android
- Sign-in options for macOS
- Sign-in options for iPhone

Use strong passwords

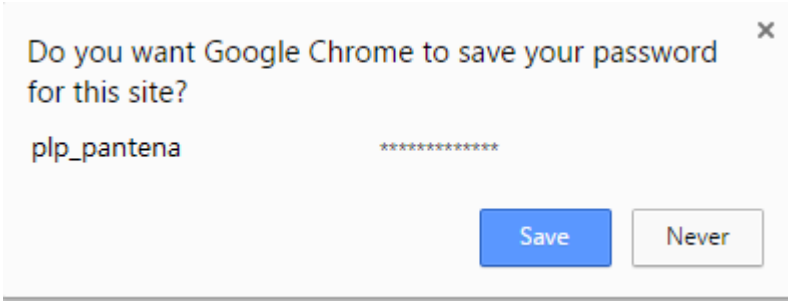
Try to avoid using predictable passwords (such as dates, or family and pet names), and don't use the most common passwords that criminals can easily guess (like 'passw0rd'). To create a memorable password that's hard for someone else to guess, you can combine three random words to create a single password (for example 'dogtreecereal').

It's really important **not** to re-use the same password for your different online accounts. In particular, use a strong and separate password for your email. If a hacker can access your mailbox, they could access information about your payments, invoices, children (and their families), as well as send emails pretending to be from you.

Look after your passwords

Of course most of us have *lots* of online accounts, so creating different passwords for all of them (and remembering them) is difficult. However, to make this easier, you can:

1. Write all your passwords on a piece of paper and keep it somewhere safe (and **away** from your computer).
2. Let your browser save your passwords for you - **it's safe for you to save them when you're asked**, provided you're OK with colleagues accessing the computer in your setting.



It's safe to let browsers save your passwords.

If more than one person is accessing your computer, you should ideally have different accounts, and different passwords for each person. Where this isn't possible, make sure you know who has access to your devices, who knows the password, and that you're OK with this. **Don't** write the password on a Post-it that's stuck to the computer, where *anyone* could access your details. For the same reasons, use a lock screen when you're not at your desk, and make sure

you change your passwords when a member of staff with access to your devices leaves.

Set up 2-Step Verification (2SV)

Many online accounts and services allow you to set up 2-Step Verification (2SV), which means that even if a hacker knows your password, they won't be able to access your accounts. It usually works by sending you a PIN or code (often sent by SMS), which you'll then have to enter to prove that it's really you. If you're given the option, it's worth taking the time to set up 2SV on your most important accounts (like email and banking) - it only takes a few minutes, and you're much safer online as a result.

Communicating safely with your families (including social media)

If you send out newsletters, social media posts, or any other communications that include photos or details of children in your care, make sure you control who can access these. For example, you should password protect newsletters so only families who have been given the password can open them. You should also check the privacy settings across any social media accounts you use, so that only the child's carers have access (the NCSC has published guidance to help you do this).

---

3. Protecting your devices from viruses and malware

Viruses are a type of malicious program that can harm devices such as computers and laptops. Once your device has been infected, this **mal**icious soft**ware** (also known as **malware**) can steal your data, erase it completely, or even lock you out of your device.

Just like real-life viruses, computer viruses spread easily. Your devices can become infected by accidentally downloading an email attachment that contains a virus, or by plugging in a USB stick that is already infected. You can even get infected from a dodgy website that you've been tricked into visiting.

This section contains tips about how to protect your devices from the damage caused by viruses and other types of malware.

Turn on your antivirus product

You should always use antivirus software on the laptops and other computers in your setting. It's often included for free, so it's just a matter of turning it on, and keeping it up to date. Most modern smartphones and tablets don't need antivirus software, provided you only install apps and software from official stores such as Google Play and Apple's App Store.

Keep all your IT devices up to date

Don't put off applying updates to your apps and your device's software. These updates include protection from viruses and other kinds of malware, and will often include improvements and new features. Applying software updates is one of the most important things you can do to protect your devices. Update all apps and your device's operating system when you're prompted. You can also turn on 'automatic updates' in your device's settings, if available. This will mean you do not have to remember to apply updates.

If you think your device contains a virus (or any other type of malware), please read the NCSC's guidance on how to recover an infected device.

---

4. Dealing with suspicious messages (phishing attacks)

'Phishing' emails are scam messages that try to convince you to click on links to dodgy websites, or to download dangerous attachments. The websites might try and trick you into giving sensitive information away (such as bank details), and the attachments can contain computer viruses that will infect your machine.

Criminals will also use other methods to trick you, such as sending text (SMS) messages, or by phone. However, the term 'phishing' is mainly used to describe scams that arrive by **email**.

This section describes how to spot the most obvious signs of a phishing email, and what to do if you think you've clicked a suspicious link.

Tips for spotting suspicious messages

Spotting scam emails is tricky, but things to look out for include:

- official-sounding messages about 'resetting passwords', 'receiving compensation', 'scanning devices' or 'missed deliveries'
- emails full of 'tech speak', designed to sound more convincing
- being urged to act immediately or within a limited timeframe

The message will often claim to be from an authority figure (like a bank, or power company). Remember, your bank (or any other official organisation) will **never** ask you to supply personal information. If you have any doubts, contact the organisation directly using their official website or social media channels. Don't use the links or contact details in any messages you have been sent.

Help your staff to spot unusual requests

Do colleagues and staff at your setting know what to do with unusual emails or phone calls, and where to get help? Ask yourself whether someone *impersonating* an important individual (a parent, manager, or member of the local authority) would be challenged. Think about how you can encourage and support your staff to question suspicious or just unusual requests, even if they appear to be from important individuals. Having the confidence to ask 'is this genuine?' can be the difference between staying safe, or a costly mishap.

Reporting suspicious messages

If you receive a message from an organisation or person that doesn't normally contact you, or if something just doesn't feel right, please report it. You'll be helping the NCSC to reduce criminal activity, and in the process, prevent others from becoming victims.

- If you've received a suspicious email, forward it to the NCSC's Suspicious Email Reporting Service at **report@phishing.gov.uk**
- If you've received a suspicious **text message**, forward it to **7726**. This is a free-of-charge service for reporting spam to your network operator.

What to do if you've already responded

If you've already responded to a suspicious message, here's what to do:

- If you think any of your accounts (including email accounts) have already been hacked, refer to our guidance on recovering a hacked account (which includes what to look out for).
- If you've been tricked into providing your banking details, contact your bank and let them know.
- If you've given out your password, you should change the passwords on any of your accounts which use the same password.
- If you've lost money, tell your bank and report it as a crime to Report Fraud, the reporting centre for cyber crime for those in England, Wales and Northern Ireland. You can contact them on 0300 123 2040. In Scotland, contact the police by dialling 101 or via the Police Scotland website.

Find out more

For more information, please visit our website (www.ncsc.gov.uk). It's full of information and guidance that will help you learn how to protect your data and devices. You might find the following sections particularly useful:

- Dealing with common cyber problems
- Protecting your data and devices
- Cyber Aware (the government's advice on how to stay secure online)

[1] Early Learning and Childcare (Scotland); Early Child Education and Care (EU). To be referred to throughout as 'Early Years'

[2] EYFS statutory framework (England); Health and Social Care Standards (Scotland); National Minimum Standards for Regulated Childcare (for children up to 12 years) (Wales); Minimum Standards for Childminding and Daycare for children under 12 (Northern Ireland).

PUBLISHED

15 March 2021

REVIEWED

15 March 2021

VERSION

1.0

WRITTEN FOR

Self employed & sole traders

You & your family

Small & medium sized organisations