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.

Int

E

Sma
and
of m
and
mec
mor

ima
ther

That
ever
devi
ther
from
why
to al
safe
and
busi
func

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

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 vast amounts of personal or sensitive information you hold on these children and their families.

Your national Early Years legislation and advice[2] and the Data Protection

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

equipment stolen, or a computer virus could damage, delete, or lock your data until a ransom is paid.

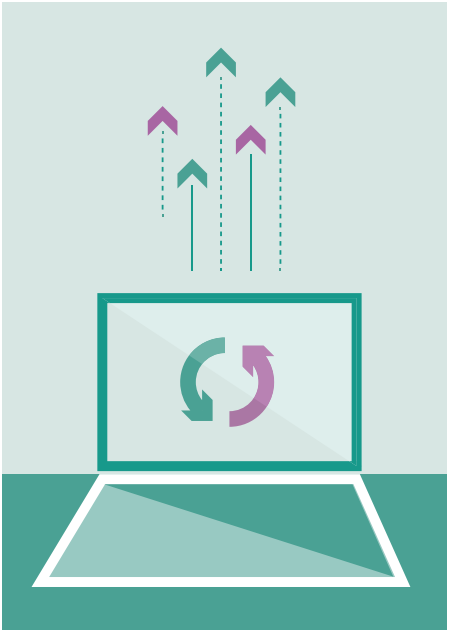
Start by identifying your most important information - that is, the information that your setting couldn't function without or that ____'

_____. Make a backup copy on a USB stick, an external hard drive, or _____'. Having made your backup, make sure you that 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:

1. A_____(iPhone, iPad and iPod Touch, and Mac).
2. G_____ (Android)
3. M_____(Windows 10) devices.



However, to make this easier, you can:

1. Write all your passwords on a piece of paper and keep it somewhere safe (and from your computer).

2. Let your browser _____ _____ for you - ' ' , provided you're OK with colleagues accessing the computer in your setting.

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. **D** ' write the password on a Post-it that's stuck to the computer, where anyone could access your details.

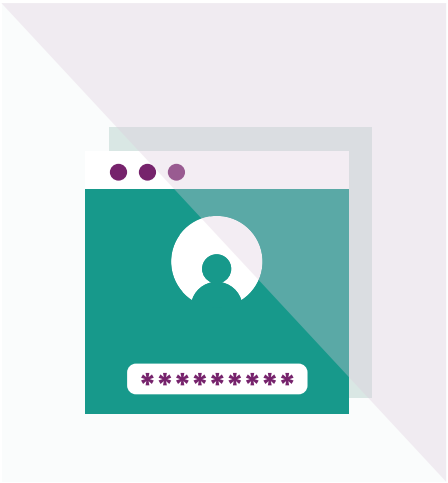
For the same reasons, use a ____ _____ when you're not at your desk, and make sure you change your passwords when a member of staff with access to your devices leaves.

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 (NC C).



3 Protecting your devices from viruses and malware

Viruses are a type of malicious

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.

Many phishing emails are now ~~ID-19~~, but criminals can 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 .

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:

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

a bank, or power company). Remember, your bank (or any

ask you to supply personal information.

If you have any doubts, contact the organisation directly using

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

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, you should 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 , forward it to the NCSC's E at @ .
- If you've received a suspicious , 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 (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 on any of your accounts which use the same password.

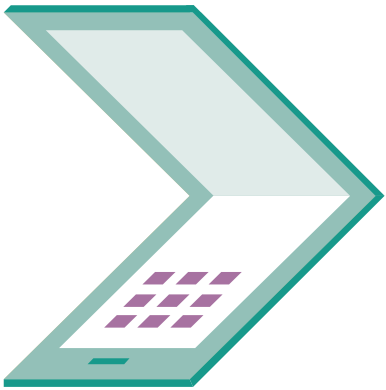
If you've lost money, tell your bank and report it as a crime to A F, the reporting centre for cyber crime for those in England, Wales and Northern Ireland. You can contact them on **0300 123 2040.** In Scotland, contact the police by dialling 101 or via the .

Find out more

For more information, please visit the National Cyber Security Centre's website. It's full of information and guidance that will help you learn how to protect your data and devices.

particularly useful

- D
-
- C A (the government's advice on how to stay secure online).



Information correct at the time of publication - April 2021

E /N C C