

Protecting information online

No online medium is totally secure - anything and anyone online can be hacked - even secret US military installations!

Your email - for example - how many times have you received messages in your inbox from friends which contain strange links? Or emails telling you that you have a beneficiary in Nigeria? Or emails giving you links to follow so you can get a tax refund? These emails are all received as a result of your email address being harvested by someone for their own purposes - and in the former case your friend's email address has been hacked and their address list stolen.

Your Facebook account - it happened to me a few years ago - I logged in and was told I was not me! It took me a few days to get back online and it was very upsetting to think that someone had stolen the information, read my personal messages, put nasty statuses on my account etc.

Cloud storage - I use cloud storage companies such as Dropbox to hold information for me. It means I can access my documents when I am out. I keep my password as securely as possible - and I log out when I leave the site so if my phone is stolen the thief cannot just click and have access to my accounts. However, no cloud is 100% secure and registration with the Information Commissioners Office (www.ico.gov.uk) is essential if you hold any information about a child on digital media.

Mobile phones - most of us use mobile phones for all sorts of things from taking photos to making observation notes to communicating with parents... there is information from Snopes on this link about how to protect photos of children when taking photos on your smartphone by turning off your GPS which I advise all members to read - <http://www.snopes.com/crime/warnings/smartphonepix.asp>.

Online software - you have no control over what happens to any details you put into online software and how they are used. You have to trust the company to maintain confidentiality, store your information securely - and not go bust and lose all your data. You also need to remember that technology will change in the future and information you input today is unlikely to be available when the child is 21 years old and putting in a claim against you for malpractice.

Working with parents - do you ask parents about their views before emailing or sending photos via your phone... contacting them via electronic devices... taking photos of their child on your phone... uploading their child's information onto an online software programme such as a photo editor or observation recording site..? It is very important that parents know what happens to information about their child, how it is protected and deleted when it is no longer useful.

There is more information about staying safe online from Childcare.co.uk here - <http://www.childcare.co.uk/information/safety-centre>.