Counter measures?

- If children are going to use Facebook, they need to be taught to do so safely and the most important aspect of this is to **check their privacy settings every time they log in,** and **parents/carers should be a "friend" on the site.**
- **Remind children that they may not take photographs of anyone without their permission, and link this with your disciplinary policy.**
- Through the ESCC scheme of work, reinforce that the sharing of credentials is not permitted.
- **This might apply to your staff too. Do you have a separate logon for supply staff with minimal privileges?**
- As part of your maths curriculum, do you cover online shopping? Could this be an interesting area?.
- **The number of applications that can be added to the modern mobile phone is growing at a rate of 200 per week.**
- Remember Tamogochis? Some of these new "apps" are just as addictive but most require some user details. Do they know what information they are sending?
- **Together, we can make E-Sussex, E-Safe.**

Further information

The East Sussex LSCB e-safety team is committed to supporting schools and member agencies.

You can book an e-safety day through the Schools Applications Support Service, and during that day, issues specific to your school can be discussed, explored and addressed.

There is a charge of £450.00 for a full day which includes a written report of the visit.

Half day visits can also be accommodated on a pro-rata basis. Evening parent visits may be possible, but we request that a minimum number of 30 is guaranteed.

You can book your day by contacting the Schools Applications Support Service on **01273 482519 (option 1)**

Or by email to:-

sas@eastsussex.gov.uk

Frequently seen online behaviours Key Stages 1 & 2

(Behaviours noted in East Sussex 2009-2010)

East Sussex County Council

eastsussex.gov.uk

Rise in mobile connected technology
A great many children now carry mobile phones to primary school. Some schools ask that these are handed in and kept securely until the end of the day, however, there is no certainty that a child would hand over their phone. Many of these phones are blue-tooth or wireless network enabled and by far the large majority of them contain cameras. There is already a rising number of iphone4s in use in primary school.

There is a bullying issue around who has the latest mobile phone and who hasn't and there is evidence that suggests photographs have been taken of staff without their knowledge.

Covert messages can be passed between infra red phones.

Some of the later GPS enabled phones allow a child's exact location to be pinpointed, and some children have this information as an add-on to their social networking sites.

Facebook.
We have to face the fact that Facebook is in widespread use by children under the age of 13. Users as young as 7 have been identified in schools and we are well past the stage of trying to ban or block the use of this product. There is significant peer pressure around having/not having this product. The older versions of social networking for children such as Club Penguin, and MushyMonsters rapidly fall out of fashion while only last year Habbo Hotel was really popular in this demographic, it is rarely seen in use now.

Evidence gained from talking to parents suggests that some of these Facebook sites are set up by adults themselves for their child in response to pressure, while some children have said that it is easy to bypass the age requirement by putting in a false year of birth. All they then need is a valid email address, which need not be theirs. A friend can click the "validate email address" button.

Identity Theft.
This may seem like a strongly worded header, but children readily admit to knowing **and using** other people's logon credentials whether to learning platforms, school networks, or even social networking sites. (This now has a name. It is called "Facebook Rape, and occurs when someone logs onto your Facebook site as you and either adds unpleasant or explicit content, or sends messages to friends as if it were the person who owns the site.) Children talk about telling friends their logon credentials, as well as family and extended family members.

It is vitally important that they do not get into the habit of using other people's credentials. Like anything else, what a child practices, they become proficient at. If they get into the belief that it really doesn't matter, they will be storing up trouble for themselves when, one day, they find that it is taken seriously.

Fraud
Another strong header! This is a child of primary age (yes, *really*) purchasing goods online using a parent/carer's account. Typically, this is where the child has discovered, or even been told their parent's logon and the parent has pre-stored bank details in the system. Some online shopping companies such as Amazon have "Buy with one-click" which does exactly what it says on the tin. You click, you buy. Instant. Children often use the excuse "My parent doesn't mind". Some children have made transactions which parents/carers have subsequently queried with Banks. Once the Bank is involved, they can take it extremely seriously. If the child is over 10, they are criminally culpable.

Insecure, online purchasing.
Some children, even at primary age, have their own bank or savings accounts, and some actually have a usable card. (Or access to it.) Children who are permitted to buy things in this way rarely check to see that the site into which they are entering their details is secure. Some payment sites say "Secure Payment", but actually are not secure at all. You need to look in the address line at the top of the web browser. An insecure site will start with http://www but a secure site will start with https://www. Only a small change, but it needs to be checked.