SCHOOLS ICT

Dos and Don’ts around e-safeguarding. Starters for 10

E-Sussex, E-Safe

Safeguarding all children in East Sussex all the time

East Sussex County Council

Provided by East Sussex County Council

E-Safeguarding is every bit as real and important as road safety, fire safety, and stranger danger.

The online world IS the real world for our children – they see little distinction – and some immerse themselves in it to the exclusion of all else.

It is also a vast area – you can't possibly be expected to know it all – and each of your children will engage in the online world to different extents and in different ways.

This is **not** a definitive guide – it can't be – but it should prove a useful starter for 10 – on both sides of the equation!

DO remember that the advantages to be gained by living, working and playing in the connected world **far** outweigh the risks, and if we all work together, parents/carers, young people, schools, colleges and local authorities, we can make sure that abuse is kept to a minimum, and we can send a clear message out "**NOT HERE!"**

DON'T underestimate the power of each other. Meeting as a group of parents/carers to talk about e-safeguarding is really valuable. Your school(s) might want to start up an e-safeguarding group. Even if they don't there is nothing to stop YOU starting one up. Your local Police Officer may be able to point you at people who can talk to your group and get you going along the right lines. The meetings can be held in a school hall, or someone's home. Communication is the key – the louder we shout when something has gone wrong, or the more energy we put behind telling everyone we know about scams, paedophile activity in the area – whatever – the better.

DO remember that it is highly likely that our children will know more about technology than we do. That can work in our favour – we can take the journey with them and use their own expertise to keep them safe.

DON'T use the same password or PIN numbers indefinitely. Children are like little sponges, and they will discover your bank card PIN, or the lock out code for the SKY+ remote. You need to change your passwords and PIN numbers regularly – at least every 90 days. This also helps to deter fraudsters, hackers, and others who like to climb inside our online world.

DO teach your child, from the earliest possible age, to realise that using technology is **not a right – it comes with responsibilities, expectations – and sanctions.**

DON'T fail to apply a sanction – if your teenager breaks the rules you have agreed with them, it **IS** ok to confiscate their mobile phone – it won't be pleasant – but you have to make sure your sanctions have an impact. If your answer is always "Yes", what value is your "No"?

DO agree your own house rules for mobile phones, games, computers, etc. Make sure your children are involved in drawing up the house rules (they will be doing this in e-safeguarding lessons in school from KS1!) Make sure that they know that there will be a sanction if they break the rules, but you can make that sanction less if they tell you about a problem rather than let you discover it.

DON'T think that it is easy for your child to tell you about things they have been doing online – no matter how close your family is, or how productive and caring the relationships are, looking mum or dad in the eye and telling you that they have been doing unpleasant things is next to impossible. It does not matter if they email you – text you, or even get a friend to do it for them. Rejoice in the fact that, whatever method they used, they told you

DO challenge them. Children will create their own myths, built around what they ***wish*** the world is like. For example, one teenager believed that if you delete the original image that was posted online, every single copy would disappear.

DON'T let yourself get painted into a "no go" corner. It IS ok for you to monitor what they do. It IS ok for you to put parental controls on their devices, and it IS ok for you to ask them to show you their online world. The moment you allow them to block you from an area of their online life, they are creating a dark area in which predators can hide

DO challenge your school(s). Schools can run e-safeguarding events for parents/carers. They can even arrange for specialists to come into school and talk with you. Many schools now offer regular parent evenings on e-safeguarding, and some of these are highly specific to one or two topics. Want to use Facebook? Fine, come and learn exactly what it is, how it earns its money, what the security risks are and how you can stay on top of them.

DON'T let your children think that access to technology is a "right" without responsibilities. You will be paying for every item of technology they use – from their computers to their mobile phones to their Kindles - they owe it to you to use it as you wish them to.

DO be a "friend" on their social media site(s). You may have to agree not to make any comments – (even to correct the spellings), but you will be able to see what friends they have admitted, and what the conversations look like. Try not to jump every time there is language there that you don't like, but **do** jump if you see conversations that look wrong. Examples of this might be:-

- A friend they and you know well, suddenly starts asking questions that they already know. This is what a hacked account can look like.
- A friend who is not the best speller in the world, is suddenly writing complex sentences and has no spelling errors. This is another indication of a hacked account.
- If your child starts to disclose "face in a place" information – this should never be anywhere near social media. People who have the right to know where your child goes already know, and strangers do not need to. So, its fine for your youngster to say "Looking forward to football

practice on Saturday". It is NOT fine for them to say "Looking forward to football practice at Selmer Park on Saturday."

DON'T ignore your feelings. You may well not have definitive proof that something has happened – but you may have a niggle that won't go away. We are becoming a society that has learned to ignore its little feelings of disquiet. We need to reawaken it.

DO say No. Just because "everyone else has it" is no reason for your child to have it as well. Doesn't matter what it is – from a new phone to an age-inappropriate game.

DON'T forget that children today have a limited sense of danger – in fact, most of their online games, rides at amusement parks, etc, encourage them to enjoy that sense of danger. In the online world, it translates as an overconfidence, and where they should be suspicious, they often accept things on face value.

DO get to understand the world of games and apps. They are not all what they seem. Some games have truly horrific graphics, and some actually encourage the player to engage in sexual scenarios up to and including rape. Some apps have "in app purchases". In some cases, these purchases have to be stopped, rather than made. (Positive marketing). People have lost a lot of money through the game and app world.

DON'T forget that as our children develop into adulthood, we need to manage their emergence as adults in the online world as well as the physical world. Pornography is all around them, and its not a question of "if" your child will see it so much as when. We must teach our children the differences between pornography and loving, caring relationships. What surprises a lot of parents is how early children start to take an interest in this kind of thing. It is not unknown for children as young as 10 to take topless or naked "selfies". Cometh the hormones, cometh the curiosity.

DO think very carefully about what technology you allow in your child's bedroom. Items that should never be up there include any device with a webcam, satellite TV and games stations. Whatever parental locks you put in place, you can be quite sure that your child will discover the passwords or PIN numbers.

DON'T let your children think that access to technology is a "right" without responsibilities. You will be paying for every item of technology they use – from their computers to their mobile phones to their Kindles - they owe it to you to use it as you wish them to.

.

DO remember that in the online world, there is usually a bigger picture. Your child may tell you they have done something online that they shouldn't have, but it may not actually be what they have said. There may also be other people involved – other children – other parents. Try to remember that it is possible to get positive outcomes for everyone involved. For example, if it transpires that your child is being cyberbullied, of course, the first order of play is to ensure their protection. But we also need to get the bully to understand their actions, and all too often it transpires that something horrible is happening to them too, and that is why they are passing on the pain, so-to-speak. Even if (worst case) it transpires that YOUR child is the one sending the unpleasant messages, there is usually a cause – anxieties around secondary school, growing up, body size, self esteem – the position can be complex beyond words sometimes. So….

DON'T let your emotions come into play if your child does ever make a disclosure. If they tell you of something, the situation is, for them, already out of control – the last thing they need is for you to get cross, either with them or whoever/whatever has been going on. You are likely to be angry/furious/disappointed/worried, or any other emotion. Try to radiate calm, listen cafefully and make sure you have the information you need. Then, remember, you are NOT in it alone. Your child's school can help.

Always Remember:-

Abusers work in darkness. They know that what they do is, literally in some cases, unspeakable. It is embarrassing to discuss paedophilia – sexual activity of children online – identity theft – fraud – being caught by a scam or a con.

When we don't talk about it, we help the abuser to do it again. They do not want us talking – they do not want you reading these words.

When we discuss e-safeguarding often, in large numbers and across different audiences we shine the light of truth and decency on the activities of those who are untruthful and indecent.

Let's agree to leave these people nowhere to hide.

So what can you do in the home?

10 simple steps to follow.

1) Know what technology you have in the home, where it is, what it does, who uses it and what for. (Don't forget the old mobile phones that could be made to work again by a technically savvy youngster.

2) Set aside some time to talk about e-safeguarding and establish a set of rules around how your children will use it. Let them write the rules – you provide the element of challenge. You are also entitled to put a couple of “non-negotiables” in there too. Such as, “This is my mobile phone, I’m paying the bill, and I am lending it to you to use.” or “If you mess up and break the house rules, there will be a consequence, however that consequence will be less if you own up, than if we find out about it.
3) Have a variety of ways they can tell you of a problem – worry box, text, email – it really doesn’t matter HOW they tell you – but it DOES matter that they do actually tell you.
4) Change your passwords – including your primary email password – often. In the home environment the following are high risk and need changing often.
    - Bank card PIN
    - Sky+ lockout PIN
    - Any online shopping account – especially if you have your browser remember your passwords and/or use “buy with one click” shopping. (Amazon, etc) Ideally, remove every password from your web browser, if someone stole your PC, they would have access to the lot!
5) Eyes and ears open. Look out for your child suddenly closing a web browser when you walk in the room – they will be more secretive as they get older, that’s to be expected – but at every occasion, challenge them on ANY idea that the internet is “private”. It isn’t.
6) When (not if) they get curious about sex – remember that they need help to emerge as healthy functional adults in the online world as well as the physical world. Porn is NOT relationships.
7) Use the News! Good news doesn’t make the news all that often especially around e-safeguarding. There will be items from time to time about grooming, fraud, identity theft, trafficking – lots of stuff – and some of it pretty ugly. Resist the temptation to change the channel. The more your child understands around how the event happened – how it started online – how it ended with a young person meeting a predator the better chance they have in avoiding it themselves.
8) Test the system. Whatever rules you have in place – how do you know they are working? How do you know that they aren’t bypassing any parental controls you have put in place?
9) Never underestimate the value of “**Computer says no.”** You can apply parental controls to mobile phones and computers. They don’t need to be logging on at 1:00am. So why not limit when their logon works? Its easy enough to do both in Windows and Mac formats.
10) Don’t let yourself believe that internet filtering will ever be 100% reliable – it wont. The more restrictions you apply to where your child can go online, the more time they will be spending at their mate’s house! Filtering is appropriate, and there’s nothing wrong with limiting websites by name or by category – but there is no such thing as a 100% effective filter. Sometimes the most innocent internet searches can result in surprises too.