E-Safety in the home

A guide for parents and carers

Let's get started.

To begin with, we need to understand just what "e-safety" means.

The term "E-Safety" means staying safe when engaging with technology that connects us with others. In hardware terms, this means computers, PDAs, laptops, mobile phones, Games consoles – both hand-held and fixed. Any device, in short, that is capable of connecting to another.

The term "E-Safety also means not only what we use, but how. It is necessary for us to know how those who would abuse the systems and the people who use them work, what the danger signs are, and how to address them.

There are two parts to it – one that is relatively easy to put in place, and one that is constantly changing.

E-safety is not "optional" – and there is no software or hardware that can magically take away the responsibility. As adults, parents, carers, teachers, we must:-

- Teach our children the risks and issues of living and working in the connected electronic world in the same way that we do for the physical world.
- Accept that, just as in the physical world, there are far more benefits than risks, but that the electronic world has its own forms of risk.

This guide is just a start on what will be a life-long journey. Technology will never stand still, and we can expect more and more devices to be connectable, and more and more opportunities to connect with other people.

This guide is written from the best teacher of all – experience. From time to time, examples are given that illustrate a point. All the examples are real-life cases.

E-Safety Starts Here!

Let's begin!

Technical e-safety (The relatively easy bit)

This means your hardware and things like anti-virus software, and wireless network security. So…

Do You Have….

	Yes	**No**	**Not sure**
An anti-virus package that includes, anti-virus, anti-spyware, anti-malware and firewall AND is it set to download and install updates regularly?			

Do you run a system scan from time to time?			
Do you have a wireless network at home AND is it protected to WPA2 standard?			
A passcode on your mobile phone, so that if you lost it no-one could access any information on it?			
A detailed list of who has access to the connected equipment you have at home?			
A way of monitoring what is going on with regard to your children's uses of mobile technology?			
A clear set of rules and expectations that have been discussed by ALL the members of your household?			
Meaningful rewards when they get it right? (For example, if your child tells you they have messed up online *before* you find out about it?)			
A meaningful set of sanctions for when they don't? (And this must *be* meaningful. Would you *really* confiscate your teenager's phone for a few days if you felt you should? Do they know you would carry through the penalties?)			
A way for them to put it right if/when they mess up? (It will be a breach of trust when this happens. For a while, it will feel uncomfortable for both you and your child. They need to be able to move on – as do you.)			
A way for them to tell you of problems OTHER than looking you in the eyes and telling you? (Sometimes, telling someone you trust and love that you have disobeyed them is the hardest thing in the world. Let them email you – text you – write you a letter….have a friend talk to you for them. The important thing is that they tell you. It doesn't matter how. NOT seeing this as hurtful is hard for parents….but then who said parenting was easy?)			

If you have all that, then you are well on the way to having the nuts 'n' bolts of e-safety sorted.

Remember, though, old equipment carries a lot of personal data about you. You need to make sure it is securely and safely deleted. A thief might not care about your

old mobile phone, but the information on it may be of interest to them – especially as mobile phones are offices on the move these days. Your emails, browsing history and even some documents may be there for all to see.

A word about Macs. Mac and their operating system have long been seen to be relatively immune to attack from hackers, malware, spyware and the more common form of attack, viruses. This is not to say that this will always be the case. Mac users should check with Apple from time to time. There are some anti-virus packages for Mac, such as the one provided by Norton. Whether or not it is needed is a personal choice.

Now the tricky part of e-safety.

Which covers not so much the hardware and software, but what people do with it.

Before we get into that though, always remember :-

Living and working in an online world carries benefits that far outweigh the risks

We now need to think a little about the "dark side" of living, working and playing online.

Why? Because if we are to keep ourselves and each other from harm, we need to understand what the risks are. Being informed is half the battle. Staying informed in a world that changes rapidly is the other half!

One of the biggest dangers is **not** talking about fraud, scams, paedophile activity, and all the other horrid things we hear about. **Not talking about them helps the**

abusers to win. Talking about it shines a large light on them and makes them fearful.

Talk to whom? Each other as groups of parents and carers, your child's school, and e-safety experts if they are invited to talk at your child's school. (If they haven't been, you could ask that the school has an e-safety day with a visiting consultant).

Fraud

This is where people try to access your money, or your personal details in order to take out loans, or impersonate you in some way.

Example:- An internet fraudster sent an email to 20,000 email addresses informing them that their bank account had been frozen. The fraudster asked for logon details and said that they would be used to reset the account. Of the 20,000 emails sent, only four people replied. They all had their bank accounts AND overdraft facilities emptied, and three of them had loans taken out in their names.

Fraud can also happen within a family, and even accidentally. When someone uses another person's logon credentials, even if accidentally, this can be fraud. In the home, the most common way in which this happens is:-

i) Sharing passwords

ii) Letting a web browser "remember password".

Example:- A young boy of 12 accessed e-bay, and placed a bid on a £23,000 car. Because his dad had let the web browser remember his password, the boy was automatically logged in, and, unfortunately, the bid his son placed was the winning bid. What made matters worse is that dad's PayPal account was set up to pay automatically at the conclusion of an auction, and was linked to a Bank Account rather than a credit card account. The result was dad ended up the proud owner of a very over-priced car, a £9,000 overdraft, and a hugely embarrassed son!

iii) Clicking on a link and then **not** checking that the link has taken you where you think it has.

Mrs X was browsing the internet and decided to follow a link to Amazon. She clicked on the link and bought an item, entering her credit card details along the way. Unfortunately, the website she ended up at was not http://www.amazon.co.uk. She had landed on a fake site. The scammer obtained her payment details and she was defrauded of several thousand pounds.

Grooming

Perhaps the one that every parent fears – a sexual predator, seeking sexual activity with a child. There are several forms of grooming, however. One is where a sexual

predator wants to meet up with a young person, and physically offend. Far more common these days, is the online sexual predator. This person tries to engage in sexual conversations or may use a webcam. They do not meet the young person, but that does not make their activities any more acceptable, or legal.

It is NOT just middle aged/old men who groom. Women can and have groomed young people, and even young people can groom young people. Forget any stereotype you have ever heard of.

Grooming can be identified very early, and some simple measures put in place can stop it in its tracks.

It is more difficult when the grooming is part of a boyfriend/girlfriend scenario. Most teenage girls, (13 – 16) prefer older boyfriends. Naturally, it is true love – and they think nothing about exchanging personal or even intimate texts or images. If the girl is under 16, the boy even asking for such images or texts may be committing a criminal offence. **Once an image is sent, the person sending it loses control of it – forever. The image may be shared, published, passed around, hacked or copied.** Few youngsters understand this.

Even adults can become subject to unwanted sexual contact and activities online.

Hacking

Hacking is often seen as glamorous – especially by young people. Breaking into a system is illegal and my carry very heavy penalties.

Example:- A young boy with Autism hacked into the US Department of Defence computers. Despite his Autism, there was an attempt made to extradite him to the US to face trial, where, if convicted, he could have served life in prison. It took over 14 years for this case to be dropped.

The most important element of e-safety that is often overlooked is YOUR comfort.

If something that someone is doing causes you discomfort or unease, then THAT alone is good enough reason to stop it. It doesn't have to be illegal for it to be unsafe.

So…… as parents and carers, you will already have a set of rules – bedtimes, household jobs – your standards of behaviour…so why not add using connected technology to them?

Have a few "non-negotiables" things that happen (or don't) purely because you, as parents say so. Children need to understand why, of course, but sometimes the answer "We are not doing that because I feel uncomfortable about it" is good enough.

Here are a few things that you might want to put in place – remember though, it is up to you to make the decisions.

1) **All computer equipment in the house is in a public place.** (Not always easy, this one, as there are good reasons why a teenager may need a quiet place to do homework where they will not be disturbed, but you can make this work for you. If they ask for that, negotiate a set of rules that they will stick to. More on "rules" below.)

2) **No webcams will ever be used in a bedroom.** (No explanation needed)

3) **No illegal downloads.** (There are plenty of sites that allow, and even encourage young people to steal music, films, software and games. However, you are responsible for what comes down your internet connection. You do not want to be an accessory to theft.)

4) **Any worries/concerns/mistakes need to be talked about.** (Try to find a non-confrontational way of letting your child tell you that they have had a problem – even if it was one of their own making – the following example comes from a real family.

   "My 13 year old daughter was acting strangely. She wouldn't say what had upset her, but she didn't want to use the computer all of a sudden. One evening, she left me a note saying that she had seen "some sex" on the internet. At first I was really concerned, but it turned out that she had been Googling for "sexy boys" and had been presented with an image of a couple making love. As images go, it wasn't that bad at all – it was just too much for her. She wasn't as worldly wise as she thought! We were able to talk about it and worked out a way that she could develop, find information she needed, but also we developed a "post-it" system so my other children could tell us of problems without having to think of that first, awful sentence."

5) **Have a family-agreed list of "Dos and Don'ts".** (Your child's school will have something called an Acceptable Use Policy – it isn't a bad place to start. All schools and workplaces have rules for the reasonable use of the internet and connected technology – having rules at home is no different really. The internet is NOT a "free lunch". There is great power to using the internet, and with great power comes great responsibility.

Know what you have, where it is, who uses it and what for is the knowledge base that you need to inform yourself about what you and your family need to do to be safe online.

On the following pages, there are forms that may help you. Don't think that you have to work through each one – but they have been developed to help focus thinking, and to guide you to asking the right questions, at the right time, of the right people.

When you are looking at the connectable equipment in your home, don't forget that old equipment can be made to work. That old Nokia mobile tucked away at the back of a drawer, might only need a Pay As You Go sim card to be functional again.

Remember also that devices rarely come with user manuals these days. They are intuitive to use, and young people will quickly discover how they connect and what they can do with the device. **It is important that you know too.**

The Practicalities.

First, you need to do an "E-Safety Audit" at home. Make a list of very single item of connectable equipment. This will include:-

- Computers/laptops/Macs etc.
- Mobile Phones
- USB drives and any other remote storage devices
- Games consoles
- Handheld games consoles.
- Televisions & Sky (or fibre optic) boxes. (Many TVs now connect to the internet as do…..
- Blu Ray players. (Many offer catch-up TV facilities, and some offer on-board gaming.
- Pagers (going out of fashion now, but there are still some around)
- Wireless routers
- Wireless USB connectors (Where two devices can be connected by plugging a USB device into them)
- Some cameras now offer "cloud storage" and can upload their contents directly to the internet.
- Any Cloud systems you subscribe to – more and more popular, especially with mobile phone providers. Microsoft Office 365 offers could-based storage. (Could-based means simply that all your files are stored by the supplier, not by you. While this does give substantial benefits in terms of the safety of your

data – it is always backed up – there can be a hidden cost here if you need more storage than you have.)

Many families discover that they have a huge amount of connectable equipment that they did not know about. (Don't forget to check down the back of the settee! Many USB sticks get lost down there.)

In terms of storage devices, you also need to think about what is on them. Always take a "worst case" view and ask yourself "If my memory stick was lost or stolen, what would the thief have access to?" Many people now encrypt their USB devices for exactly this reason. You can buy encrypted USB storage, and for your more sensitive material – bank letters, family photos etc, this is a good idea, but there are free methods of encrypting USB devices. One of them is http://www.truecrypt.org/

Take your time doing the audit. It is time well spent.

You may find the form on the next page helpful.

E-Safety in the home

What equipment do you have that connects to the internet?	**Where is it located?**
Who has access to what device?	**What old/unused connectable equipment do you have & where is it?**

Connectable equipment:- This means any device that can connect to something else. It may be wireless, a mobile phone, iPad/Pod/Phone, games station – ANYTHING that has, or has the potential for an internet connection AND/OR connects via the mobile phone network including 3G.

Location:- It matters where the equipment you have is located in the home. Some things that may be of concern are:-

i) Games stations in bedrooms.

ii) Webcams in bedrooms.

iii) Old mobile phones (many of which have personal data on them) that you can't account for.

Who uses what? This is a vital area to consider. As adults, we may want to restrict what our children can access on the internet. Allowing them totally free and unrestricted access can place them and you at risk. It is important to understand just what they can and cannot do. Children today are highly IT literate – they can learn or work out your passwords in the blink of an eye!

It is also important to know whether or not your children are accessing age-inappropriate games, some of which have highly violent and disturbing graphics. There have been academic studies that have proven a link between such games and aggressive behaviour, both in home and school.

Children with connected games stations in the bedrooms can easily be online into the early hours without you knowing.

The Survey

The purpose of this survey is to help to indicate where you may want to make some changes to the way you and your family use computers or access the internet. There is no single "right answer", however, this survey will help you identify areas where you may be at risk.

1) **Does each member of your family need a password to access the internet? (Yes ☐ No ☐**

2) **Do you EVER ask your computer to "remember your password? (Yes ☐ No ☐)**

3) **Can other members of your family log onto your shopping sites? (Yes ☐ No ☐)**

4) **Do you ever check what your family is downloading from the internet? (Yes ☐ No ☐)**

5) **Do people from OUTSIDE your family access your internet connection or computers?** (This may be friends or children's friends) **(Yes ☐ No ☐)**

6) **Do you REGULARLY check your bank statement or credit card statement for items that should not be there? (Yes ☐ No ☐)**

7) **Does everyone in your family know how to identify a fraudulent email? (Yes ☐ No ☐)**

8) **Does your family have a set of agreed rules for using the internet and mobile phones AND do you review it regularly? (Yes ☐ No ☐)**

9) **Do you discuss e-safety in your family regularly – particularly when you hear about e-safety items in the news.** (Paedophiles, internet fraud, etc)? **(Yes ☐ No ☐)**

10) **Do you know which agencies can help you if you or your family had a serious concern regarding the internet, online games or mobile phone abuse? (Yes ☐ No ☐)**

Score 1 for every "Yes" answer and 0 for every "No" answer.

0 – 3 = You need to talk about e-safety in your home urgently.

4 - 6 = Doing well, but some areas need further work.

7 - 8 = Not bad at all! You are well on the way to becoming e-safe.

8 – 10 = Some minor adjustments needed, but well done!

E-safety Changes.

As the technology and applications become ever-more sophisticated, uses and abuses do too. There is never a single "right answer", however, there are things you can do. Here are the most common ones.

1) **NO bank or building society will EVER ask you to confirm your details by email. ANY email asking you to do so, or telling you that there is a problem with your account is likely to be fraudulent. Do nothing – but if you are worried, phone your bank/building society.**

2) **Sadly, many chain letters seeking to raise money for what appears to be a "good cause" aren't doing that at all. You should make your own decisions regarding charitable donations, and not respond to emailed marketing.**

3) **Ideally, everyone in your home should have a password for accessing the internet, or home computers. PASSWORDS SHOULD NEVER BE STORED IN ANY INTERNET BROWSER.**

4) **Knowing what is being downloaded can save you a lot of trouble. There are internet sites that encourage young people to break the law with regard to copyright. Remember – YOU are responsible for what comes down your internet connection.**

5) **There has been some difficulty with so-called "free" apps. Some users have found that downloading the App might be free, but using it certainly isn't. Make sure you understand if there are any costs involved – this may require you to read a lengthy and very boring "Terms of Use" document.**

6) **As well as paedophiles, there are a large number of people who would like to gain access to your personal details. Teaching young people what unacceptable questions look like in internet chat rooms is time well spent. Youngsters want to take responsibility for themselves early these days, and some fraudsters and paedophiles are very plausible.**

7) **It can be embarrassing when an item on child abuse appears on the news – particularly grooming. It is important that you do not paint yourself into any "no-go" areas of conversation. The more you talk about how and incident happened, the better able your child will be to avoid it themselves.**

8) **Knowing where you can go for e-safety help and advice is important. Your child's school can often help, or they can access training for you and your family. There are also places online where you can go for help**

and advice. www.thinkuknow.co.uk http://www.childnet-int.org/ http://www.education.gov.uk/ukccis/

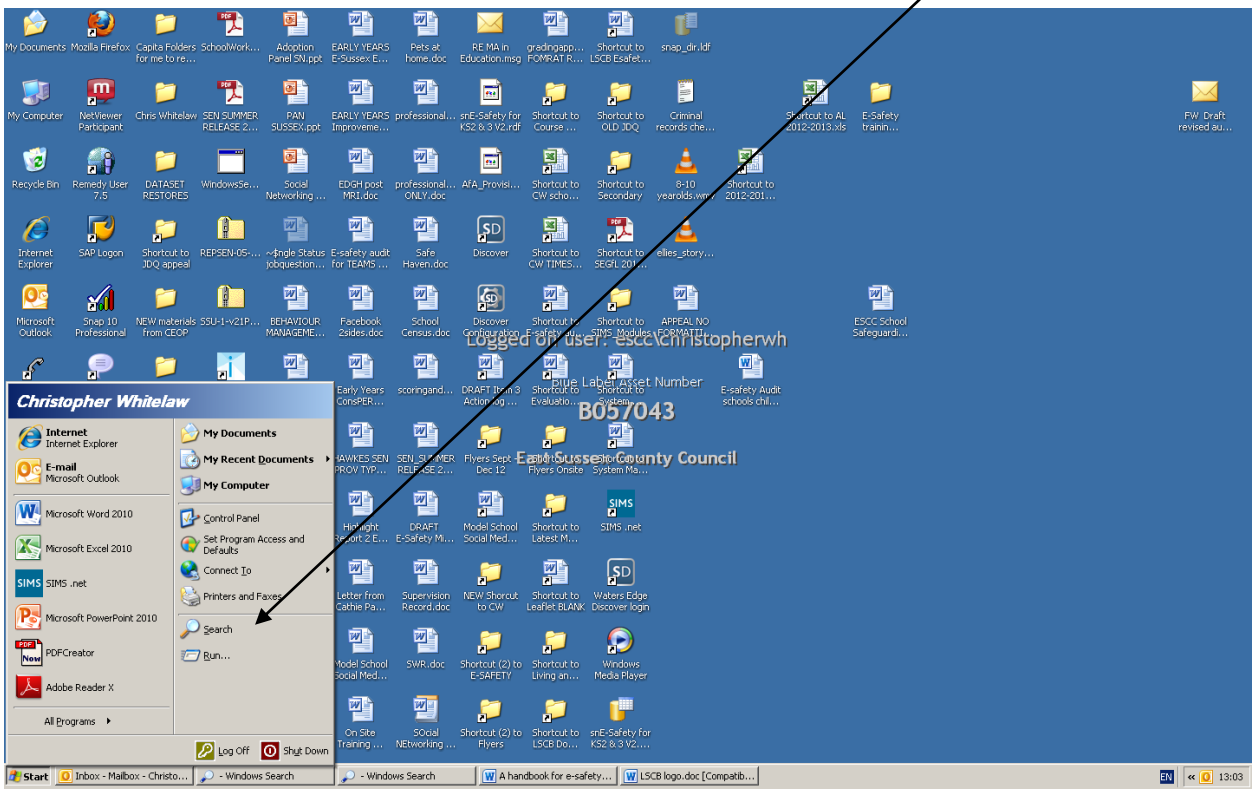
9) **Remember that children are very "technology aware". They have a natural curiosity, and will often think they know when they are safe or not. There are many myths around – and new ones come along all the time. (See next page)**

10) **ABOVE ALL – make it "ok to tell". If your child is worried about something they have done online, it is vital that you find a way that they can tell you about it. Sometimes looking you in the eye is impossible for them – but there are other ways. Please remember, that when a child or young adult has a problem, to them, the situation is already out of control – they do not need you out of control too, no matter what has been going on.**

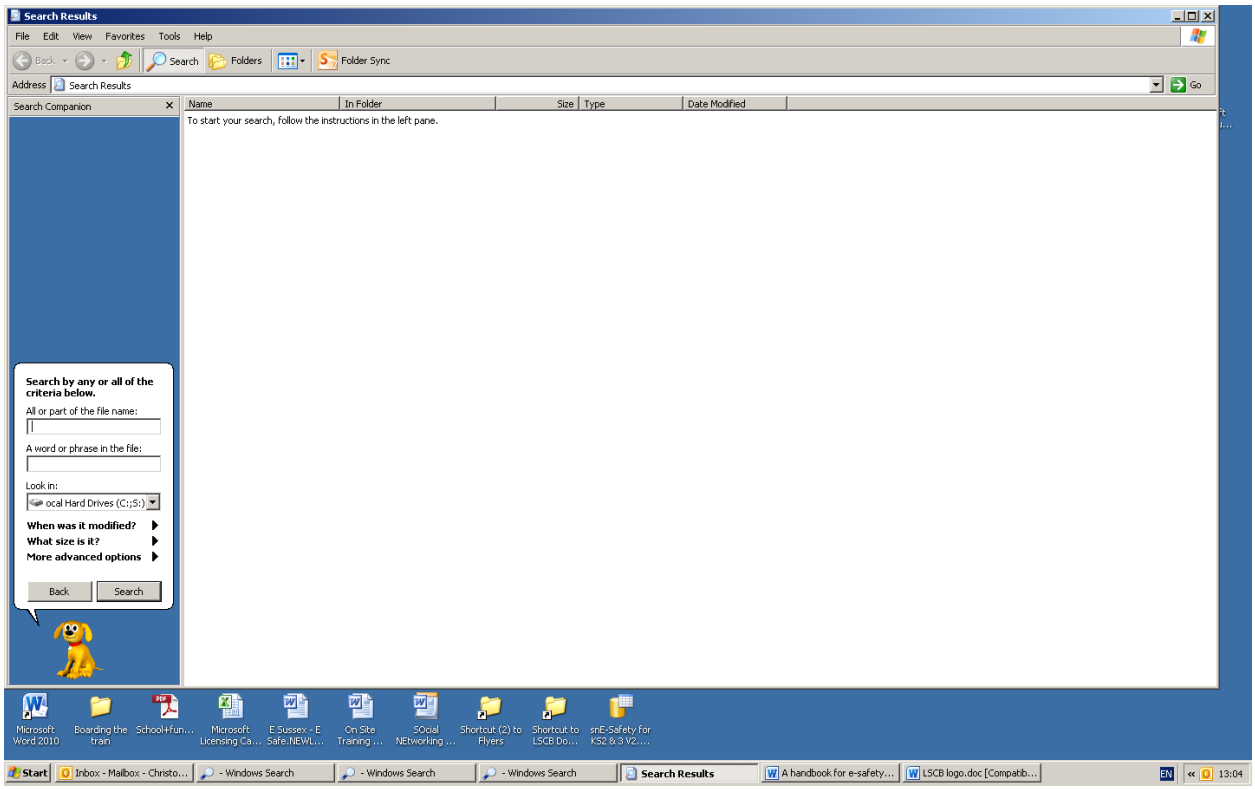
Checking computers? How do I do that?

From time to time, it is handy to make some simple checks into what is on your computer, and in Windows, it is simple to do this.

Go to the START button in the lower left corner, then find SEARCH



This may bring up one of two versions of the search facility. The easiest to use is the “SEARCH COMPANION” – if you have this option then select it.



IN the box marked “ALL OR PART OF FILE NAME”, you can type ONE of the following, depending on what you want to check.

*.jpg – brings up all photographs stored on the computer.

*.doc – brings up all Word documents

*.pub – brings up all Publisher documents

*.mvi – brings up stored movies – (please note there are several movie formats)

*.wmv – as above, a movie file.

In Macs, look at the “finder” icon.  It is usually on the lower left of the “dock” (this is where the various icons that control the machine are kept. Most users have it at the bottom of the screen similar to a Windows taskbar.

Ideally, you will be set up as an administrator for every computer (including Macs) in your home. You will need to be able to check all the user’s files. Fortunately, Mac includes a “log” that can be useful for checking activity. See the booklet on **User Accounts in Mac** for more details.

Also worth checking from time to time is the internet history file. This might vary a little depending on which browser you use, however, under **TOOLS|INTERNET OPTIONS,** click on the **GENERAL**, tab, then find **Browsing History|settings|view**

There may be a lot here, but more interesting is if it is empty – that indicates someone is clearing the internet history. You may want to find out why.

Again, in Macs there is a “log” file that is most helpful to computer administrators for looking at where a user has been on the internet.

Top Ten Internet Myths (As disclosed by children and young adults)

1) **"It's easy to hide on the internet."** (Yes and no. While it is easy to lie – even set up a totally false profile - every electronic contact leaves a trace and even if identities are hidden, it is easy for appropriate agencies to track what was going on, and who was involved. Internet Service Providers have a statutory duty to assist the Police with their investigations.)

2) **"If I post an image online, I can delete it, and any copies anyone has made are deleted too."** No! Just NO! This is not true. Once you post an image online, you lose control of it forever. A few simple rules will help:-

   i) **NEVER post any image online that you would not show to your strictest relative**

   ii) **Only ever post minimal-resolution images online – that stops people trying to read background information, or enhance/change the image.** Some organisations such as Facebook use the images you post online, in fact they may well gain intellectual ownership of the material you post – read their Privacy Statement!

3) **"Cyber bullying is just something that happens."** Yes, it does – and so was some of the worst things in human history. We are not powerless, and we can stop unpleasantness such as cyberbullying. Cyberbullying is nasty. It is also hurtful, damaging, potentially lethal, and may well be illegal, particularly if hateful, religious or racist comments are made. (Some people were prosecuted and jailed not because they took part in the riots in London – merely because they egged them on using social media.)

4) **"Bidding on e-bay is a laugh – no-one knows you have done it".** To bid on e-bay you have to log in – that means there is a trace. Placing a bid is a legal contract – a statement that if yours is the successful bid, you will buy the item. Some parents have found that their bank account has been emptied because their child had access to their e-bay account. (Incidentally, for your protection, it is far better to link PayPal to a credit card than a bank account.)

5) **"Everyone I know has sexy pictures of their girlfriends on their mobile phones.**" And if the girl in question is under 16, it may well constitute a criminal offence – FOR THE BOY! When relationships break up, it is not uncommon to find these images posted all over the internet, often tagged to make them easy to search for. A dumped boyfriend can be every bit as hurt as a dumped girlfriend.

6) **"Everyone downloads music for free – or makes copies of their CDs and uploads them"** If this is really happening, then "everyone" is committing theft. The Federation Against Copyright Theft (FACT) in the UK has become very

active as they themselves have engaged in new technology. It is now far easier to track down people who steal music, films, videos and software.

7) **“Hacking is well-cool.”** And it is also seen as glamorous – and it is also a criminal offence. Hacking means breaking into a computer system, usually, although not exclusively, by pretending to be someone else. Expect the most severe penalties – especially if you have hacked into the US defence department’s computers –they, and others, really don’t like it!

8) **“Everyone shares passwords – so what?”** So you are impersonating someone else when you do this, and also committing a criminal offence for which you can be prosecuted. Do you have areas of your online life that you want to be “private?” How about your Facebook account, for example? How would you feel if someone took control of it away from you and started to post truly appalling material while pretending to be you? Lemmings all jump off cliffs – does that make it the right thing to do?

9) **“I use my mum’s credit card when I need to top up my mobile phone.”** And if you do it without her actually being there and entering the numbers herself, you are committing fraud. Mum may also be at risk if the bank finds out. There are rules and regulations to owning and operating a bank account. One of them says that account holders must not allow anyone else to access the account. Banks can and do impose financial penalties on people who let their accounts be used by others. Banks are also increasingly good at spotting when an account is being used like that. All it takes is one phone call to mum by the bank asking her what the date of a particular transaction was for them to know what is going on. Letting it become widely known that you have access to your mum’s credit card might also put you at risk pf physical bullying as well as cyberbullying.

10) **“Getting revenge on someone on the internet is easy – you can ruin their life!”** If you are in the position of wanting to hurt someone, and you want to give the police a lot of hard evidence, then go ahead, use computers or the internet. Every electronic contact leaves a trace. No exceptions. The material you post may also be illegal in itself. If the person you are attacking harms themselves as a result of something you did you can be charged with that too.

    There is also plenty of case evidence where internet users have been prosecuted for inciting hatred. During the riots in London, one person encouraged others to go and join in – he was sent to prison. Where racially-motivated hate is concerned, the penalties are really stiff. If you have a relationship problem, there are far better ways of dealing with it than going online. Relationships fail – you can either accept that and move on, or carry the baggage with you.

As Parents and Carers, Ideally….

- You want your whole family with you on the internet e-safety journey. The more openly it is discussed, using news items to start discussions off where you can, the safer and more informed everyone is.
- Remember, too, that children's needs vary in accordance with their age and intellectual maturity.
- Don't allow any area of e-safety to become a "no-go" area. That is often where problems start and develop.
- The more empowered you and your family are, the better.
- Having a password for everyone is no bad thing – your children will be used to that from school or college.
- With new operating systems it is easy to set up child accounts on computers with appropriate restrictions on what they can do with it and where they can go online. Some even offer the parents usage reports – you get a system-generated email every week or so telling you what websites have been visited and what searches made.
- Operating system designers take e-safety seriously, and have realised that the more "goodies" they build in, the more popular their system becomes with parents.
- Don't forget the mobile phone either – they aren't really mobile phones anymore – more like offices on the move. You may have imposed reasonable internet access restrictions on the family computer(s) but that is of little use if you give them an unrestricted access mobile phone when they go off to secondary school. Mobile phones are the subject of another publication in the "A guide for parents and carers" series.
- When you buy a new games station or ipad, increasingly, these days, you are invited to enter some payment information during the setup procedure. Make sure you know why this is being done, and what limits (if any) you can set. Sometimes, it is possible to complete the setup without entering payment details, but sometimes this is not made clear. If you don't want to enter your card details, try just clicking on "next" and see what happens. It may well be that you can continue the setup.

Finally, enjoy the online world, it offers wonders aplenty – together, we can shine a light on those people who wish to make the internet a dark and scary place.

Together, we can make E-Sussex, e-safe.

Intentionally blank for your notes.