E-safety information

Mrs Birtchnell – E-safety and computing curriculum leader
West Borough Primary School

Introduction:
The speed at which the internet is changing the world we live in. We saw the sites which are becoming overwhelming popular, and the increasing amount the online world is integrated into daily life – both for adults and children.

Even as little as 10 years ago the internet was not integrated in this way into so many aspects of our daily lives. 10 years ago, there wouldn't have been a need for a session such as this. Today, social media is all around us; it is making it simpler to communicate and make contacts, opening doors to new exciting opportunities for creativity and education.

We need to remember, children are natives in this online space, most are unaware of life without iphones, games consoles or Google. They feel confident in using new sites and technologies, moving from site to site with ease, exploring and engaging in fun activities.

70% of parents of children aged 12 – 15 feel that their children know more about the internet than they do. (Ofcom media literacy 2011)

If you look at what's happening in social media today and the skills your children are developing there are some tremendous opportunities for them and it's important that we help our children take every advantage of them. Then we will explore the negative things about being online, because some of the risks children face are very real.

I hope to equip you with the knowledge and awareness needed to feel confident to talk about these technologies with your child and take the action required to protect them.

This will enable you to go home and do what you do best… support them in their growth and development as their parent or carer

Online Learning:-

Now, let's start to think about the positive aspects of being online.

Communication skills – communicating is one of the prime reasons for children going online. They are talking to others, sharing their lives, building connections and friendships. Children have the opportunity to build and maintain connections and communication with a far wider group of people than has been possible in the past.

Computer skills – children are engrossed in technology at a very young age. They see older siblings or family members using computers and Iphones and quickly copy them. How many of your children before the age of 5 knew how to operate your phone or laptop? These skills are then developed and enhanced over time. As technology plays an increasingly important part in all of our lives so does the importance of being able to use it effectively.

Creativity – Through building online spaces and avatars (online characters), online games encourage you to be creative. By using their creativity in this environment children are learning new skills, exploring their imagination and opening their minds to new opportunities.

Research – Children research online. They turn to search engines and other online tools to find out about an interest or piece of history. They are learning how to find and understand complex information from a range of sources and apply this knowledge. Being able to navigate the internet in this way is going to be an increasingly important skill, both in daily life and at work.

Confidence – The internet gives you the ability to be anybody you want to be and try new things. In the real world a child may struggle to build friendships, but online they can be a 'popular' king of an online universe (literally!).

Money management – Who here has bought their child online currency or an online game membership for their child? Children build accounts online and use the currency gained or bought to buy key pieces of online merchandise, such as pets or furniture. Gaming companies suggest that by doing so, they are learning money management. A key lesson is that you can't buy everything you want and you must work for it. What do you think?

Topics covered in this document:-

The internet and the technologies used by your children can sometimes feel intimidating, especially if you are not internet savvy, use the technologies regularly yourself or don't know anything about a particular site. Where do you start?

Firstly, don't be scared! Though technology does move fast there are simple things you can learn to help protect your child online. Most importantly, remember that rules you set your children in the real world can also apply in the online world. You **CAN** take control. I hope that the basics which we'll learn today will help you do this.

The topics we will be discussing in this session are as follow:

- The possible risks posed to your children in the online world
- The types of technologies they are using
- The ways you can protect them in these online spaces
- Where you can go for more help and advice – remember today is just a taster. You will need to go home and look into the needs of your child and apply what we have discussed

CEOP:-

CEOP (Child Exploitation and Online Protection) is the UK's national lead agency for the protection of children online.

Set up in April 2006, they have been working hard to protect children from harm, and to date (April 2011) have arrested over 1,164 sex offenders and safeguarded over 1,038 children.

Through its education program, Thinkuknow (which has been seen over 8 million times), CEOP create engaging films and materials, which [schools, youth groups], such as ours, use to educate and empower children to protect themselves in the online environment.

One of the aims of the Thinkuknow program is to teach children that if they are ever worried about someone they're talking to online they can report them to CEOP using the ClickCEOP button. As a parent you can also report directly to CEOP through this button, which you can see here on the screen.

If your child has experienced sexual or offensive chat while online which has made them feel uncomfortable, or someone is trying to meet up with them, you can report this. This contact may have happened in a chat room, on a message board, instant messenger or via a social networking site. It could also be on a mobile phone, through a games console or computer. It could be messages, images or conversations over webcam. To report inappropriate contact with your child on the internet go to CEOP's Safety Centre by clicking the ClickCEOP button or visiting www.ceop.police.uk:

If you press this button you are taken through to this safety centre, packed full of help and advice about all types of online issues. Never be scared to report to CEOP, they understand the complexities of monitoring children's online usage and how easy it is to be contacted or even tricked online. They are there to help and protect your child and hold the offender to account.

Search engines can make our lives easier. They make sense of the chaos of the web, linking us to the sites we need, when we need them. Google, Bing and Yahoo are all search engines and some of the most visited sites in the world.
With a world of information at their fingertips, it's easy for children to stumble across things that might upset or disturb them. They might also come across sites which aren't suitable for their age.
Remember, this can happen by accident and, while most parents and carers trust their children online, children are naturally curious. They may search 'rude' words, without thinking about the results they might get.
A simple way to help stop your child seeing things they shouldn't is to change the 'search settings' on search engines. These aim to prevent the search engine bringing up results which might not be suitable for children.
Note: No filter is 100% accurate and sometimes content slips through the net. Ensure that your child knows to come and tell you if they see something that upsets them.
CEOP advise parents to watch these films with their child in the comfort of their own homes. It is a great way to open dialogue about their online life and shows them that you understand the complexities of the issues faced. Hopefully they will feel secure in approaching you if they feel out of control or are uncomfortable with something they see online.

So...we have already talked about the skills learned through online activities and the opportunities these create, but what about the not so nice things that can happen online? What can go wrong, what are the risks?

Grooming and unwanted contact There are people online who will try to contact children and build a relationship with them.. They may use information they've gained about a child from a social network profile or from chatting to them in a forum or gaming site. They may communicate with a child for some time online trying to build a relationship of trust. The overall aim will be to meet with them and abuse them in the real world.

Children need to understand that it is easy to be tricked online and that people are not always who they say they are. If your child has been contacted by someone who has acted inappropriately towards them, remember you can report directly to CEOP using the ClickCEOP button.

Cyberbullying Cyberbullying is when somebody bullies another through the means of technology. The majority of this bullying takes place peer to peer and it can be difficult to locate a perpetrator. Some children set up fake profile pages on social networking sites with mean content and ask the whole school to join. They may use text messages to pester and harass a child through the night or exclude them from playing online games.

This type of bullying is hurtful and sometimes goes unnoticed. Every school must have an anti- bullying policy and take this form of bullying very seriously. It is sometimes difficult to locate the bully, due to the anonymity of the internet. However it can be tackled and must not be ignored as the effects on the child affected can be devastating. .

The important thing to remember about cyberbullying is that it leaves an evidence trail. This can be useful when attempting to find and challenge the perpetrator. If your child receives a hurtful text or email tell them they should not reply, but also that they should not delete it. Always ask your child to keep messages and save copies of content wherever it may be, as when they are ready to tell someone, such as you or a teacher, they have something to work from. You should also learn how to save a copy, as you may stumble across such content. To save evidence of a malicious social network profile, or anything on your computer screen,- press print screen on your key pad and then paste the image of your screen into a word document.

Removal of content – If the content has been posted online, only the service provider or the person who posted it can take it down. If you can't

get the person who posted it to take it down then you should report it to the service provider. For instance, if it happened on Facebook, you will need to report the issue directly to them through the reporting button next to the photo, page or comment.

Harmful content/ Illegal sites Who here has seen something online they wish you hadn't? It could be something you have stumbled across or a link that was sent to you by a friend. How likely do you think it is that your child has had the same experience?

There is material online that is not appropriate for children to be viewing. This material could be pornographic or homophobic, it could promote self harm or anorexia. Some content may even be illegal. In the real world it would be difficult to come across or gain access to this material, however online it can be found through open research or sent as a link or virus.

To stop children viewing or stumbling upon inappropriate content, you need to put filters onto the laptop, computer, games consoles and mobile phone that your child uses. This will go a long way towards ensuring that inappropriate material is blocked. It is not 100% fool proof, but it's a start and will give you some piece of mind.

Privacy / Digital Footprints When we teach children about personal information, we explain that this could be your school name, home address, a status update on where you are going to be on Saturday night, inappropriate photos, or just about anything that if it got into the wrong hands, could be used against you or used to locate you. By placing this type of information into an online space, you are leaving digital footprints behind. Try typing your name into a search engine such as Google or Bing tonight and see what you find, then do the same with your child's name.

Tell your child to think before they share anything online and to only post comments and images that they wouldn't mind showing you or a member of the family.

Websites and technologies:-

We are now going to take a look at some of your children's favourite sites and technologies. We only have time for a few, so please go home and talk to your child about the ones they use and apply the knowledge you have learned in this session to educate them on keeping safe.

Can anybody name their children's favourite sites or technologies?
[most probably they are…. Minecraft, Facebook, Twitter, Foursquare, Moshi Monsters, Bin Weavles, Tumblr, World of Warcraft)

Let's talk now about social networking. It has exploded into our lives, with many of us feeling the pressure to join in or miss out.
Who here has a Facebook profile? How many of you are friends with your child on a social networking site?
Sites such as Facebook, Twitter and Youtube are all social networks. They allow you to reconnect with long lost friends and communicate in ways we never dreamed possible.

With more than 750 million users worldwide and 695,000 status updates a minute, Facebook is leading the way in social networking. It changes its functions often, but here are some of the main ones you need to be aware of:

- This is the 'About me' section, which is not mandatory to fill out – check your child's profile to see what personal information they have shared. CEOP advise that children use their real date of birth when signing up to the site (as if you are under the age of 18 you have more security added to your profile), but to hide this from the main page. They should never share their location, school or date of birth in this section.
- Status updates are very popular with children. They will update umpteen times a day, telling all their friends what they are up to and what they are thinking. Children should never share their exact location in their status updates, especially if they have people they don't know on their site. This is the equivalent of having 100's of people in one room, standing on a stage and broadcasting what you have to say.
- Friending is one of the main reasons people use Facebook. Finding people you know and adding them to become your friend can be fun.

You have a window into people's lives and can find out information that wouldn't have been easily available before. But this works both ways. Children should only add and accept people they know and trust in the real world, not friends of friends or someone they have just met in another online space. These people will also have a window into their lives!

- Photos - sharing photos is a great way of showing all your friends how fun your weekend was or your latest holiday snaps. Children need to think before they take and post an image. Some children share too much, such as, pictures of them in their school uniform, of the family home or even bikini or topless shots … Children should remember that once they've posted something online they've lost control of it. Images can be copied and pasted into any other space without their permission.
- Setting up events on Facebook couldn't be easier. With all of your friends in one space, why would you choose to go anywhere else when setting up a birthday or get together? Events you set up can be set to private, and this will mean that only the people invited will see the details. This is advised for all adults and children. Do you want everyone to know where you are going to be on Saturday night?
- Facebook has a private messaging function, which means you can talk one to one with any of your friends if they are online at the same time as you. It is known that offenders online will attempt to talk privately. Children should only talk to people they know.

If your child does have an account, there are ways to help protect them. Keep your child's and your own profile safe by:

- Clicking on 'account 'in the top right hand corner
- Privacy settings
- Look at the range of customizations you can make. As a minimum ensure that it is set to 'friends only' and that all of their friends are people they know and have met in the real world.

The risks associated with social networking are…

- Sharing personal information
- Unwanted contact from strangers
- Unhealthy networking – Visiting groups and pages which are not appropriate for their age

- Inappropriate content – this is an adult site and the content is self generated.
- over usage – How many times a day does your child check their Facebook account?

Talk to your child about their social networking accounts. Ask them to be "friends" with you and take these simple steps:

- Security settings need to be set to "Friends only"; that includes comments, posts and photos
- These **"Friends"** need to be people they know and trust in the real world
- **Content** - Only post content and photos they wouldn't mind showing you!
- Try your very best to be "Friends" with your child on Facebook
- Learn how to report an issue directly to Facebook

Facebook for Pre Teens

Has anybody here been pestered by their child to have a Facebook or social networking account, but feel they are too young?

Can anybody tell me how old you need to be to sign up to Facebook? **The answer is 13.**

If you allow your child to use sites such as Facebook, you are not breaking the law, you are breaking the site's terms and conditions.
There is no right or wrong answer here. It would however feel wrong to allow an underage user on the site and to let them run freely. The content and security settings are adult in their nature and young children need to be moderated particularly closely.

CEOP believe that education in this area is key. Though there are good reasons why children are restricted from accessing sites like Facebook, we do not want to push these young users underground. If we throw them off or ban them from the site, there is a possibility that they will set up one anyway and use it without your guidance. The most important thing is for you to be involved in their internet use.

Discuss with your child the age at which it would be appropriate for them to be on social networking sites. The transition between Primary and

Secondary school seems the most popular. Whatever age you decide your child can go on social networking sites make sure you have discussed some of the risks, such as creating a digital footprint, and then stay involved in their use, mentoring them to become a responsible user.

If you are going to allow your child to join, think about:

- Helping them set up their profile
- Adding your email as the main contact (where possible)
- Setting the privacy settings to "friends" only and ensure these are friends from the real world and known by you
- Showing them a CEOP safety resource which outlines the risks (www.youtube.co.uk/ceop/jigsaw)
- Adding the Click CEOP button – type Click CEOP into the facebook search box.
- Checking in and keeping updated with the content they are posting and receiving in this space

If you have any questions which relate directly to Facebook, please visit their family safety centre for help and advice – www.facebook.com/safety

Gaming:-

Can anybody tell me the names of the gaming sites their child uses?

As you will know, gaming is very different to how it used to be. Put Pacman and Tetris to the back of your mind and think MMORPG – this means that a game is a Massively Multiplayer Online Role Playing Game, which in short means that a site can have unlimited users and the game **never** ends.
Many gaming sites allow you to play and communicate against other users all over the world.

One of the most popular ways for children to kill time is on their games consoles. Put your hands up if you have a console in your home? Keep your hand up if it links to the internet? The majority of these do, which means your child can link to other users, talk and play against them.

How long do you feel is an acceptable amount of time for your child to be spending online of a school evening? There is no specific guidance set around this subject, so as a parent you need to set boundaries and rules on acceptable usage. Ensure they have enough time to do their homework of an evening and spend some time doing a technology free activity. A screen should not be the last thing they see before they go to bed!

Some of the risks which your child can encounter on a game console are:

- Inappropriate content – other users typing or saying (over headset) abusive language
- Unwanted contact – other players wishing to play against you that you do not know or trust
- Overuse – children can spend a large amount of time on games consoles and internet based games.

Tips

- Make sure the laptop, computer or games consoles are not located in your child's bedroom. They need to be in a family space so you can see when they are using them and who they are talking to, possibly through the VoIP (headsets) that many of these games have.

- The majority of all games consoles link to the internet, please do not forget this. Treat them and set safety rules just like you would on a laptop or PC
- Open up communication – talk to your child about the sites they are using and why they like them.

- Explain that people lie online and they are not always who they say they are
- Explain that people can be mean and don't always have their best interests at heart
- Ask them to never give out personal information
- Set parental controls – visit the service provider's website or CEOP's parents' pages for help
- Set time limits on how long they can game for. Allow time for non-technology based activities and allow an hour screen free time before bed

PEGI (The Pan-European Game Information age rating system) was established in 2003 in order to help European parents to make informed decisions about the games children play.
Just think of them like age rating systems for films. If the game has 3+ it is suitable for a player of 3 years and over; if the game has 18+, you need to be 18 or over. Do not let your child tell you otherwise. I have heard stories of children telling their parents that this is an ability level! As well as the age ratings, there are symbols to go alongside. These will give you a better indication of what the game is about. Some games such as Grand Theft Auto will have all of these symbols.
I would ask you to be careful with the types of games you play with and in front of your child.
Please visit www.pegi.info for more information

Talking privately is a normal and natural thing to want to do. Adults would possibly meet someone for a coffee or call their friends, but Children like to IM, Facebook chat or BBM.

Risks:-

Windows Live Messenger or IM (Instant Messenger) is a private chat service which anyone can use as long as you have a hotmail account. One of the exciting things about IM is that it has the ability to use a webcam.

You will recognize if your child uses this area, by the amber flashing bars at the bottom of the screen.

In a recent survey (Ofcom 2011) 52% of 11-16 year old internet users say they find it easier to be themselves online, 47% talk about different things online than offline, and 27% talk about more private things online than when with other people face to face.

Offenders know this and use areas such as IM and others to groom children. They know that in this area they can chat privately and build relationships and trust over time. The key message is simple: your children need to (just like the advice for social networking), only have friends that they know and trust in the real world. They must never give out personal information and if they feel uncomfortable, must report. There will be advice on reporting at the end of this session.

Webcams – As I mentioned IM has webcam capability and so do many of the new and up and coming sites, such as Chatroulette and Tinychat. Webcam gives the other person an insight into your personal life and home. Children need to be aware of the type of information that is visible in the room they are in (not the bedroom) and remove anything that could make them vulnerable. Full name on certificates, pieces of work from school etc..

Make sure you turn the webcam away from the room or off when it is not being used. There are ways of switching these on remotely, without you knowing!

BBM – please put your hands up if your child owns a Blackberry phone?

One of the main reasons for teenagers insisting on having this phone is down to its messenger capability. They can link with friends who also have a Blackberry and chat for free and in private. This can mean that they never turn off BBM and spend hours messaging. Make sure you set boundaries and downtime for all technologies.

These "friends" need to be real world friends; it is also advisable that you ask your child to only place photos and updates on their BBM that they wouldn't mind showing you.

Tips

- Ask your child to never accept communication from people they don't know and trust in the real world
- Inform them that giving out personal information can be dangerous. They need to treat personal information such as the school they go to or their location like their tooth brush and not share it with anyone else!
- Ask them not to webcam with people they do not know from the real world and turn the webcam off after use!
- Teach them how to report a problem and to delete people that make them feel uncomfortable

Mobiles:-

How did we ever live without them? They're a great way to keep in touch with friends and family and, if you've got a smartphone, check in on your Facebook when you are out and about. There are apps for just about anything and the possibilities for entertainment are endless. Think of mobiles as mini computers, this way you will understand that safety measures need to be in place.

What do you think your child uses a mobile phone for?

- Talking/chatting
- Texting
- Going online
- Taking photos
- Sharing their location

The majority of these phones are fitted with GPS, which is fantastic when you are lost and need Google Maps assistance as it can pin point you on a map and tell you exactly where you are and how to get to your destination.

However, this function is now being used on sites such as Facebook and Foursquare. You can now tell people your exact location by 'checking in'.

So if you "check in" this is shared on your social network profile and all of your 'friends' can see where you are. Let's remember not everyone is who they say they are online. People can tag you in places, which you may not want to share with everyone you know. You can protect yourself and your

child by changing settings in the privacy settings area. It has never been more important for your child to know who they are taking to and the information they are sharing.

Some of the **risks** are as follows:

- Images can be taken and uploaded. With the introduction of digital media, we have lost the time to process what we are going to do with a particular image. Within seconds it can be taken and uploaded online.
- Location
- Personal messaging
- Over Usage

Tips

- A good time to allow your child to have a phone is when it is needed. i.e leaving the house alone – starting secondary school
- Before buying a mobile find out what functions it has – Internet, private messaging, built in applications
- Set parental controls where required – talk to the service provider
- Do not allow mobiles in the bedroom at night; insist that they need to be charged overnight in **your** bedroom or the kitchen

If your child wants to access a new site or use any new technology you're not familiar with you should always consider the following before allowing access:

- What's the purpose of the site? What's fun, why does your child like to use it, what functions are available? Picturing sharing? Chat? Webcam? IM?
- Is there a section for parents/carers? If not, then this causes concern. If the site is aimed at children, information should be available for parents
- Learn how to report a problem to the site. This way if your child has any issues, you can assist promptly
- If sharing information is involved, can it be made private? See if the site has any security settings; can you make it private?
- As a parent can you set any extra controls? Such as time limitations, how much money is spent, emails sent to your account

The best way to understand any site your child uses is to join yourself, sign up as yourself and see what all the fuss is about!
Always remember that nothing online is 100% safe – there is always the potential for misuse either by adults or children.

Parental controls:-

Parental controls have already been mentioned, but put your hands up if you have already set any parental controls on your child's devices? Can anybody tell me the type of content it blocks? How they can help you as a parent?

It is never too late to put these restrictions in place. You can set specific times when the internet is not available, time restrictions and even have the restrictions lifted when you know the children are in bed.

Please remember that once these settings are set, it does not mean that you are 100% "safe". Some content may slip through the net and you will need to report it to your service provider. Moderation and open communication is most importance.

For more information please visit the parents' website or call your service provider (BT, Talktalk Sky etc...) and see what packages they provide, some of which are free. There are also some you can pay.

To find out more google 'parental controls'. Remember, the internet is available through many devices. Make sure your child is safe by controlling their phone, games consoles, laptops and PCs.

I advise that you go home and talk to your children about the sites they use, open up communication channels. Explain that you understand why they enjoy using these sites; however you would like them to use them safely.

You may trust your child, but do you trust everyone else on the internet? Keep them safe by being a part of their online life, become friends on Facebook or game against each other on their favorite site. Set boundaries, rules and block illegal and inappropriate material.

Cyberbullying:-

For further support about cyberbullying you and your child can visit a fantastic site called www.cybermentors.org.uk . They are a charity who specialise in this subject area and give a safe place for your child to talk openly about their feelings with other young children.

Once again, visit ClickCEOP for to make a report if someone is being inappropriate with your child online.

And lastly, inform your child that if they have an issue and they feel they cannot talk to anyone they know, they can always call Childline in confidence (it won't even show up on the phone bill) – 0800 1111

Lastly, these are a few steps for you to go through, use it as a tick list; it's a good place to start.

- I have asked my child to show me sites they use
- I have asked my child to set the security settings on all the technologies they use
- I have asked my child to only accept people they know and trust in the real world as online "Friends"
- I have set safe settings on our computer/laptop and set filters on my child's smart phone
- My child has agreed to tell me if they are worried about something online