Online Safety at Blean

Tea and Topics – Online Safety

The internet is amazing. Children can play, learn, create and connect - opening up a whole world of exciting possibilities. But with the digital world changing all the time, how can you make sure your child's staying safe?

Our Commitment to Online Safety

We recognise that children's opportunities for using the internet within their homes is increasing rapidly and that unless parents are made aware of the dangers, their child may have unrestricted access to the internet. We help our parents to plan and understand appropriate supervised use of the internet at home through Tea and Topic sessions, newsletters and online safety events.

- All staff have DBS, copies of Online Safety and Safeguarding policies, regular training, sign AUPs.
- All children start a new term of Computing with online safety sessions, and sign AUPs
- E-Safety Crew, ambassador training, displays and ethos at Blean.

What is Online Safety?

- Online Safety supports our children in staying safe in the virtual world. It is important that we equip children with the skills they need to keep themselves safe so they can experience the internet positively and responsibly.

Safer Internet Day 2018

The children have been learning about Online Safety to help them understand how to keep themselves safe when using the internet and other electronic devices.

- Assembly by ‘E-Safety’ crew
- Learning Walk from local policeman
- Progressive tasks EYFS to KS2 to explore key skills within a meaningful context

-Opportunities to talk and share experiences of Online Safety

-Artwork from each class to respond to ‘Connect Share and Respect’ theme

Online Safety and the Early Years

Children start using computers from a very early age and are increasingly using the Internet more and more whether it is at home, in school or on a games console. With this in mind, Internet Safety and knowing how to protect themselves online is essential.

Before you click, click, click…
You need to think, think, think…
And TELL
someone!

Task

- List the knowledge and skills our children will need to have to be equipped to use the internet and digital technologies safely and responsibly.
- What the internet is,
- Personal information,
- Password protection,
- Digital footprint.

The Internet of Things (IoT)

- It’s important to be aware of technology, toys and internet safety. That’s because over the next few years, millions of objects will be connected to the internet. You might have already bought an internet-connected gift for your child, so it’s important to be aware of the potential risks.
- The Internet of Things, sometimes called the IoT, refers to everyday objects that connect to the internet. Internet of Things devices can be activated using voice commands and can be controlled remotely using a smartphone app. Lots of these devices are also Bluetooth-enabled, meaning they are able to connect to nearby devices, without having to connect to the internet.
- Internet of Things examples include:
  - smart speakers, such as Google Home and Amazon Echo
  - wearables, such as Fitbit and Apple Watch
  - smart meters measuring household energy consumption.

What is the Internet of Toys?

- Along with the devices above, many toys now connect to the internet. This is sometimes referred to as the Internet of Toys. These products include:
  - toys with voice and/or image recognition, such as Hello Barbie™ and Furby Connect
  - app-enabled robots, drones and other mechanical toys, such as Dash and Dot.

What are the risks of internet-connected devices?

- Because IoT devices can feel unobtrusive in the home, you may not realise they pose the same security risks as more conventional devices, such as smartphones and tablets. This means you could be more relaxed about your security when using them. In reality, these devices collect personal data, often both audio and visual. These devices might also be vulnerable to hacking, as there are no safeguards or security standards for internet-connected objects.

8 tips for keeping your family safe when using internet-connected devices

1. Read the manual

Check the guidance provided by manufacturers. Product information often comes with new devices or can be found online. This will give you some idea as to how the device collects and shares data.

2. Be app aware

Many Internet of Things devices require downloading an app. You should check the privacy settings and permissions of any apps you download, as well as the product itself.

3. Consider buying brands

Buying a recongised brand is likely to offer greater security than cheaper options, although there have been data breaches with some of the most popular IoT toys. Reading reviews online will help you understand the digital safety of a product.

4. Use parental controls

Many products have parental controls or child-safe modes as standard. These limit search abilities and access to paid-for services.

5. Check your connections are safe

It’s important that your internet router is secure. Most internet service providers have security features, so you may want to consider switching these to safe mode. If the device has Bluetooth, set it to ‘undiscoverable’, otherwise you may unintentionally share data or allow hackers to take control of the device.

6. Be password protected

Make sure all passwords are changed from their defaults. The use of strong, unique passwords is essential to protecting you and your family online

7. Talk to your child about online safety

With any internet-connected device, whether a smartphone or toy, it’s important to speak to your child about staying safe online.

8. Ask for advice

Parental Controls

- Innocent searches sometimes reveal not so innocent results. So if you're worried about what your child is searching for online, who they're talking to or what they're seeing, we can help.

- Parental controls are software and tools which you can install on phones or tablets, games consoles or laptops – and even your home broadband.
- You can also use them to help you block or filter the content your child sees when searching online. And family-friendly public WiFi can help when you're out and about.
- Parental controls are also available to help you to:
  - plan what time of day your child can go online and how long for
  - stop them from downloading apps they're too young for
  - manage the content different members of the family can see.
- So whatever your child is doing online, there's a way that you can help keep them safe.

Mobiles and tablets

- Lots of mobiles and tablets come with settings that can help you manage what your child can and can’t see or do online.
- When using parental controls, make sure to check things like location settings and what information your child is sharing with others.
- You can get more information about setting up controls on different devices from the UK Safer Internet Centre and mobile providers such as O2, Vodafone, Three and EE.
- And don’t forget to talk to your child about what they’re doing online and how to be Share Aware.

Home broadband

- Your internet provider may offer a free filter so you can control the content that you and your family see. You'll need to manually set-up any device connected to your home broadband.
- How you do this depends on your provider and you'll need to access your home router or hub. It's really easy and simple to do. You can get guidance from UK Safer Internet Centre and Internetmatters.org on how to do this or you can give our experts from the O2 & NSPCC helpline a call **0808 800 5002**.
- Don't forget if your child uses their device away from home, then they'll be able to connect to public WiFi which might not have the same settings.
- If your child accesses the internet at home through 3G or 4G rather than using WiFi then they won't be subject to the parental controls.

Games consoles

- Most games consoles are internet-enabled. Which means your child can go online and chat with other players or make in-game purchases.
- Like with mobiles and tablets, the controls on your games console help you to manage what your child can and can’t do.
- Some devices allow you to:
  - set up different profiles for each family member
  - deactivate the internet
  - turn off chat functions to stop your child from talking to strangers.

Film, music and TV

- You need to think about parental controls when watching films or TV and listening to music.
- Smart TVs and services like Netflix, iTunes, BBC iPlayer and YouTube have settings that allow you to control who sees what.
- Take a look at Internetmatters.org or UK Safety Internet Centre for more advice

Search engines

- Make sure the content that your child sees online is appropriate for their age by using the controls available in search engines like Google and Bing.
- Setting up filters like Google SafeSearch helps to protect your child from seeing inappropriate or adult content. Or you could use a child-friendly search engine like Swiggle and Safe Search UK.

WiFi and being away from home

- The controls you've set up on your child's device and your home broadband won't apply if they use 3G or 4G, public WiFi or log on to a friend's connection instead.
- Public WiFi is often available when you're out and about. But it's not always secure and can allow children to search the internet free from controls.
- Some venues and businesses offer family-friendly WiFi. When you see the family-friendly WiFi symbol it means that when you connect to the WiFi there are filters in place to stop children from seeing harmful content.
- Talk to your child and agree with them what they can and can't do online. And if they're visiting friends or family remember that they might not have the same controls set up.

Apps and privacy

- It can be hard to keep track of all the apps and social networks that are available and what they do. Some apps let young people send messages to each other or store personal information.
- Others are for playing games or having fun. Whatever they do, remember you can talk to your child about their privacy settings.
- Net Aware is a parent's guide to the apps and networks that children are using and has more details about controls and privacy settings.

Talking to your child – openly, and regularly – is the best way to help keep them safe online.

You might find it helpful to start with a family discussion to set boundaries and agree what's appropriate. Or you might need a more specific conversation about an app or website your child wants to use or something you're worried about.

Explore sites and apps together

- Talk about what might be OK for children of different ages. Ask your child what sites or apps they like. Write a list, and look at them together.
- Be positive about what you see, but also be open about concerns you have: "I think this site's really good" or "I'm a little worried about things I've seen here".
- Talk to your child about what you think is appropriate – but also involve them in the conversation. Ask what they think is OK for children of different ages – they'll feel involved in the decision-making.
- Be aware that your child might talk about friends who use apps or visit sites that you've decided aren't suitable. Be ready to discuss your reasons, but recognise that they may not agree with you. Listen carefully for the reasons why.
- Go through a final list of sites you both agree are OK, and work out when you'll next discuss it.

Ask about things they might see online which make them feel uncomfortable

- Talk about things they, or their friends, have seen that made them feel uncomfortable:
- Be specific. What exactly made them feel uncomfortable and why? Is it people or animals being hurt? Nasty comments about others?
- Link these to things in the real world, and explain that you're always here to protect and help them online and off.
- Reassure your child that they can always talk to you about anything that makes them feel uncomfortable.
- Show them how to report or block on the sites and apps they use. Use Net Aware to find out how.
- Tell them you'll help them to report anything upsetting they've seen, or to deal with online bullying.

Talk about how they can stay safe on social networks

- Ask your child if they know:
- where reporting functions are
- how to block someone
- how to keep information private.
- Show them how to do these things. Use Net Aware to help you.
- Talk about online privacy, and being Share Aware. Explain that online behaviour – including sharing personal information – should mirror behaviour in person.
- Explain that talking to strangers isn't always 'bad', but they should always be careful about what they share and sometimes people aren't who they say they are.

Reassure them that you won't overreact – you're just looking out for them

- Explain that you understand the internet is a great place to be and that you're just looking out for them. Tell them they should speak up and not keep secrets if something is worrying them.
- Reassure them that you're interested in all aspects of their life. Say that you'd like to talk about stuff they've seen online, sites and apps they visit, and that you'll share the things you've seen too. Recognise that they'll be using the internet to research homework, for example.

Be Share Aware: talk about what's OK, and not OK, to share online

- Talk to your child about what 'personal information' is - such as email address, full name, phone number, address and school name - and why it's important.
- Explain simple ways to protect privacy. For example, avoiding usernames like birthdates or locations that give away too much information.
- Discuss images and photos, and what might be appropriate. Help your child understand how photographs can give people a sense of your personality, and that sharing the wrong kind of image can give the wrong impression.
- Explain that it isn't easy to identify someone online. People aren't always who they say they are, so don't share personal information. If it's someone who genuinely knows your child, they shouldn't need to ask for personal information online.
- Tell your child that if they're in any doubt they should talk to you first.

Talk about their online world

- We talk to children about crossing the road, bullying and speaking to strangers. But what about staying safe in the digital world?
- Having regular conversations about what your child is doing online - just like you would their day at school - is the best way to keep them safe.
- You'll be able to spot any problems, encourage them to come to you if they’re worried and make sure they know what’s ok to share online - and what’s not.

3 tips to help start the conversation

1. Explore sites and apps together and talk about any concerns.
2. Ask your child if they know how to stay safe online.
3. Talk about personal information and what to share online.

Create a family agreement

- Creating a family agreement is a great way to start talking about online safety.
- It'll help your child understand what behaviour is appropriate when they're online. And they'll know who they can turn to if they are ever worried about anything they see or do.

Explore popular social networks, apps and games

- Children and young people use social networks to:
- share photos or videos
- chat with people via messages, voice calls or video
- film and broadcast videos via live-streaming
- play games
- You've probably heard of Facebook, YouTube and Snapchat - the most popular networks used by 11-16 year olds. But what about Omegle, Musical.ly and Periscope?
- To learn more about children's favourite social networks, their suggested ages and how to use privacy settings, visit Net Aware.

Task

- **A Social Media Profile** - A fictional profile that may reflect websites our children are interested in, and occasionally have access to. Can you spot any Online Safety issues?

FriendPad

Search

Sal Jane Smyth
Born on **14th May 2002**
Lives in **Hipsley**
Mobile: **079 738 261**

Find me on...
Chirper: **SJSmyth**
Picgram: **SalJane**
Snapbook: **SalJaneSnaps**
Messages: **SJSmtyth1405**

1,064 Friends
Add Me!

Likes...
- **Cats** (especially my cats Danny and Donny)
- **Photography** (LOVING my college course!)
- **Fifth Direction** (best band in the world ever!!!)

Dislikes...
- **Little brothers** (Billy is soooooo annoying!)
- **Baked beans** (yuk!)

One hour ago... 2
Having an amazing time at Coasterland in Great Yarmouth. If you're nearby, send me a message and we can meet up!

Yesterday... 5
Can't wait to visit Coasterland tomorrow. Looking forward to catching up with **Jay** and **Sam**. We've been chatting online for a few weeks and it will be great to finally meet them!

Jay:
Should be cool **Sal**! Meet you at the entrance at 11am!

Sam:
Don't forget your camera!

Sunday 28th June... 97
Snapped this amazing pic outside my house yesterday.

Photo Location: **28 Hipsley Avenue, Hipsley**

Saturday 20th June... 23

Task

- https://www.esafety.gov.au/education-resources/classroom-resources/challenge/cybersmart-forever

- **Read the following scenarios and decide what to do with the image. Circle the emoji that best describes the action you should apply to the image.**
- **POST**– This is a photo you would be happy for anyone to see
- **SHARE** – This is someone else's photo that you could share
- **DELETE** – This is a photo that should go straight in the trash

Screenshots: what you need to know

- Screenshotting is when someone takes a copy of their screen and stores it as a picture. This means that messages and images which are thought to have been sent privately can be recorded and shared without the sender knowing. It's important to make your child aware of the risks of screenshotting.
- Anything on a screen can be screenshotted. This includes apps like Snapchat which allow you to send a photo, video or message that 'disappears' after a certain amount of time.

What are the risks?

- Screenshotting means that images and messages can be stored and shared with others, without the sender knowing about it. This can play a role in bullying where pictures, messages and videos can be used against the sender.
- We also know that screenshotting is sometimes used in sexting incidents, where a young person has shared a sexual image with someone else. That person can then screenshot the image, and share it on. It's important for young people to be aware that taking, storing and sharing sexual images of someone under 18 is illegal, even if the image is of themselves.

Can screenshotting be helpful?

- Whilst there are risks, screenshotting can be helpful sometimes. For example, it can be used to record evidence of online abuse or bullying to show teachers or parents.
- However, screenshots should not be used to record evidence of sexting, as taking a screenshot means you are creating a sexual image of a child, which is illegal.

How can you keep your child safe?

- Talk to your child - make sure your child understands that people can screenshot their messages, even when they think they’re having a private conversation. Remind them that they can speak to you if anything upsetting ever happens to them online.

Task - The Digital Footprint

Think for a moment about your digital footprint. Ask yourself ...

- Where do I go on the web?
- Am I learning new things as I journey on the web?
- Am I a member of any online sites?
- Have I connected with like-minded people, people with whom I share interests and information?
- Have I ever published information on the web?
- Have I contributed thoughtful or reflective or positive or helpful feedback or comments on any forums or blogs?
- What sort of image am I leaving behind - in photos, comments, views and opinions displayed online?

Now, think about who might track or follow or explore your digital footprints?

Why might they do this? What might they find?

Friends

Employer –
current and future

Family

Colleagues

Identity Thief

Employees

Teachers

Stalkers

Model a positive digital footprint on the World Wide Web.

- Social media profiles - interesting, 'clean', demonstrating your positive personality
- Website or Blog - create a website about something you're interested in or passionate about. Write interesting articles, post ceative pictures, etc.
- Blog comments - comment sensibly and positively on other websites or blogs that are about things of interest to you
- Shared photos - share your creative, artistic, sensible photos on photo-sharing sites such as Flickr
- Youtube - create your own Youtube channel and post videos you've created about your interests or passions
- Newspapers - contribute articles to your local newspaper or comment on articles of interest
- College newsletter - achieve at school in a positive way to be mentioned or contribute articles to the College newsletter
- Book reviews - contribute reviews to relevant sites