

ONLINE SAFETY PACK







Things to consider...

Keeping safe

- How safe is our personal information?
 - Do we have strong passwords? Eg capital letters, symbols etc
 - Do we all have usernames that don't reveal our full names?
- Have we considered parental controls which would be right for our family?
- Have we discussed online friendships and whether we can trust them?
- Do we need a family email address?
- Who will we talk to if we feel uncomfortable about anything we have seen or heard online or on a mobile phone or gaming device?
- When is it okay to download files, games or apps?
- Have we checked the reviews and ratings for apps and games?
- Which websites are okay for us to use?
- Should we open links from people we don't know?

Social networking

- Do we know the age requirements to be on social networks?
- Who can I post photos of online?
- Do I know why it is important for my accounts to be private?

Gaming

- Which age rated games can I play?
- Am I aware of why PEGI is important?
- Can I play online with people I don't know?

Positive online behaviour

- How can I be a good friend on the internet?
- What will I do if I receive frightening or bullying messages?

Healthy lifestyle

- How long can we spend online?
- Do we spend the same amount of time enjoying our offline activities?
- Where can we use our devices around the house?





Suggested ideas for an agreement with younger children.

We agree to...

I will use my tablet for ____ mins a day

We will make sure the children's favourite games are bookmarked for them to get to easily

Who is responsible for this?

Isabel and Phoebe

Mum and dad

Suggested ideas for an agreement with pre-teen children.

We agree to...

I will tell mum and dad when I see something that worries me

We will put parental controls in place but review it as the children grow up Who is responsible for this?

Jack and Tom

Mum and dad

Suggested ideas for an agreement with teenage children.

We agree to...

I will make sure all my social networking sites are private and that I only accept requests from people I know

We won't post photos of our children without their permission

Who is responsible for this?

Jane, John and Ben

Mum and dad









The internet – an inspiring and positive place

The internet is an amazing resource which enables children and young people to connect, communicate and be creative in a number of different ways, on a range of devices. However, the internet is always changing, and being able to keep up to date with your children's use of technology can be a challenge. You may sometimes feel that your children have better technical skills than you do, however children and young people still need advice and protection when it comes to managing their lives online.

Issues that your child may encounter on the internet will vary depending on their age and online activities. We have grouped potential online risks into these 4 categories.

Conduct:

Children need to be aware of the impact that their online activity can have on both themselves and other people, and the digital footprint that they create on the internet. It's easy to feel anonymous online and it's important that children are aware of who is able to view, and potentially share, the information that they may have posted. When using the internet, it's important to keep personal information safe and not share it with strangers. Discuss with your child the importance of reporting inappropriate conversations, messages, images and behaviours and how this can be done.

Content:

Some online content is not suitable for children and may be hurtful or harmful. This is true for content accessed and viewed via social networks, online games, blogs and websites. It's important for children to consider the reliability of online material and be aware that it might not be true or written with a bias. Children may need your help as they begin to assess content in this way. There can be legal consequences for using or downloading copyrighted content, without seeking the author's permission.

Contact:

It is important for children to realise that new friends made online may not be who they say they are and that once a friend is added to an online account, you may be sharing your personal information with them. Regularly reviewing friends lists and removing unwanted contacts is a useful step. Privacy settings online may also allow you to customise the information that each friend is able to access. If you have concerns that your child is, or has been, the subject of inappropriate sexual contact or approach by another person, it's vital that you report it to the police via the Child Exploitation and Online Protection Centre (www.ceop.police.uk). If your child is the victim of cyberbullying, this can also be reported online and offline. Reinforce with your child the importance of telling a trusted adult straight away if someone is bullying them or making them feel uncomfortable, or if one of their friends is being bullied online.

Commercialism:

Young people's privacy and enjoyment online can sometimes be affected by advertising and marketing schemes, which can also mean inadvertently spending money online, for example within applications. Encourage your children to keep their personal information private, learn how to block both pop ups and spam emails, turn off in-app purchasing on devices where possible, and use a family email address when filling in online forms.

There are real advantages in maintaining an open dialogue with your child about their internet use. Not sure where to begin? These conversation starter suggestions can help.

Ask your children to tell vou about the websites and apps they like to use and what they enjoy doing online.

Ask them about how they stay safe online. What tips do they have for you, and where did they learn them? What is OK and not OK to share?

Ask them if they know where to go for help, where to find the safety advice, privacy settings and how to report or block on the services they use.

Encourage them to help someone! Perhaps they can show you how to do somethina better online or they might have a friend who would benefit from their help and support.

Think about how you each use the internet. What more could you do to use the internet together? Are there activities that you could enjoy as a family?

What can I do right now?			
Maintain an open dialogue with your child and encourage them to talk to you about their internet use: for example who they're talking to, services they're using, and any issues they may be experiencing.			
☐ Create a family agreement to establish your children's boundaries, and your expectations, when on the internet.			
Give your child strategies to deal with any online content that they are not comfortable with – such as turning off the screen, telling an adult they trust and using online reporting facilities.			
Consider using filtering software to block unwanted content. In addition to filtering, remember that discussion with your child, and involvement in their internet use, are both effective ways to educate them about the internet.			
Encourage your children to 'think before you post.' Online actions can impact not only yourself but the lives of others. Content posted privately online can be publicly shared by others, and may remain online forever.			
Understand the law. Some online behaviour may break the law, for example when downloading or sharing content with others. Be able to recommend legal services.			
Familiarise yourself with the privacy settings and reporting features available on popular sites and services.			
If your child is being bullied online, save all available evidence and know where to report the incident, for example to the school, service provider, or the police if the law has been broken.			
Familiarise yourself with the age ratings for games and apps which can help to indicate the level and suitability of the content. Also see if online reviews are available from other parents as these may be helpful.			
Set up a family email address that your children can use when signing up to new games and websites online.			
Encourage your children to use nicknames (where possible) instead of their full name online, to protect their personal information, and create strong passwords for every account.			
Set up a PIN or password on devices to help protect personal information.			
Sign up to our Childnet newsletter at www.childnet.com .			

 $Help\ make\ sure\ that\ your\ children\ know\ how\ to\ stay\ safe\ online,\ by\ using\ our\ SMART\ Rules\ for\ primary\ aged\ children,\ or\ 5\ Tips\ for\ Teens.$

5 SMART Rules for primary aged children:

Safe: Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password.

Meet: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

Accepting: Accepting emails, messages, or opening files, images or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

Reliable: Someone online might lie about who they are and information on the internet may not be true. Always check information by looking at other websites, in books, or with someone who knows. If you like chatting online it's best to only chat to your real world friends and family.

Tell: Tell a parent, carer or a trusted adult if someone, or something, makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

5 Tips for Teens:

Protect your online reputation: use the tools provided by online services to manage your digital footprints and 'think before you post.' Content posted online can last forever and could be shared publicly by anyone.

Know where to find help: understand how to report to service providers and use blocking and deleting tools. If something happens that upsets you online, it's never too late to tell someone.

Don't give in to pressure: if you lose your inhibitions you've lost control; once you've pressed send you can't take it back.

Respect the law: use reliable services and know how to legally access the music, film and TV you want.

Acknowledge your sources: use trustworthy content and remember to give credit when using other people's work/ideas.

Further advice and resources:



KEEPING UNDER FIVES SAFE ONLINE



Children love using technology and are learning to navigate websites, online games and consoles, and touch screen technology like tablets and smartphones from a younger and younger age.



Latest Ofcom research has shown that 81% of 5-15 year olds have access to a tablet at home and almost 40% of 3-4 year olds and two thirds of 5-7 year olds go online. We know that children need support in these environments, to get the best out of using the internet, and there are real advantages in making sure that children are supported in their internet use right from the start.



These eight frequently asked questions will provide you with useful information and tips that you can put in to place at home, to help keep your youngest children safe online.



Where do I start?

The best way to keep your family safe online, and to understand your children's internet use, is to use the internet together. Active engagement and conversations with your children are key. Be positive and embrace the technologies that young children enjoy and look for family activities or games. Take time to explore the games and services that your children are using, or want to use, and look out for any safety features that may be available. This will give you a better understanding of the different ways that children are engaging with technology and help you to feel more confident.

Should I set any rules?

In the same way that you set rules for most areas of your children's lives, establish your expectations regarding online activities. Creating a **family agreement** (www.childnet.com/have-a-conversation) is a useful step, which might include time spent online, sites that can be visited, and behaviour expected; remember, what's right and wrong offline is also right and wrong online. It's a great idea to agree these rules from the outset, so that you and your children are aware of their boundaries.





How can I supervise my child?

Placing your computer or laptop in a busy part of the house e.g. the living room or kitchen can be helpful. This can make it easier for you to be involved in their technology use. But remember, the internet can be accessed from a number of portable devices, for example smartphones, games consoles and tablets. Portable devices may allow you to ensure your children are using them where you can see them and your children can still be supervised. To find out more about the internet capabilities of smartphones, gaming consoles and other devices, check out our Parents' Guide to Technology (www.saferinternet.org.uk/parent-tech).

How much time is too much time?

Children can be enthusiastic users of technology. The challenge can be to harness this enthusiasm and ensure a balance, so that the use of technology does not negatively impact on other important areas of young children's lives. There are some strategies that can be used to help manage the time online issue, such as agreeing time limits or using time limiting tools, designating weekly times to use the internet together, or removing portable devices from your child's bedroom at night to avoid tiredness.





Are there tools to help?

There are free parental controls and filters available, to help you set safer boundaries for your children, but you will usually be required to set them up. Your internet service provider (such as BT or TalkTalk) will provide free filters to help block age inappropriate content for children, and on the UK Safer Internet Centre website you can watch video tutorials (www.saferintenet.org.uk/parental-controls) that show you how to find and set these up. All Mobile phone operators (such as O2 or Vodafone) also provide such parental controls for free. The websites of device manufacturers (such as games consoles) should also outline the controls to which you have access.

Filtering options can be found within websites and services themselves, for example on YouTube or 'safe search' settings can be applied to search engines such as Google or Bing. There are even some services adapted for children (such as the YouTube Kids and BBC iPlayer Kids apps). Parental controls can be password protected, so it's advisable to choose a strong password and not share it. Parental controls and filters are a good starting point but it is important to recognise that they are not 100% effective. They are a great help, but not a solution, and work best in combination with parental supervision and engagement, to help your children understand how to stay safe online. As children grow and develop, so do their online needs, therefore you may want to periodically review your parental controls to accommodate this.

What advice can I give my child?

Education is the best tool that a child can have, so discuss with your child the importance of telling an adult immediately if someone, or something, upsets them online. Make sure that your children know that they can come and talk to you (without necessarily getting into trouble) if they see anything that worries them on the internet, and encourage them to feel confident enough to do so. Other immediate strategies to deal with unwanted content or contact could include; switch the screen off, close the laptop, exit the website, or turn the iPad or phone over and put it down.

Younger users may be distracted by advertising and pop ups and with just a couple of clicks, or a spelling mistake, may find themselves on a different website. Children are naturally curious and will innately push boundaries. Bookmarking sites or creating a 'favourites' list is a simple way to help your children find the content they want without having to search the internet for it. It is also important whilst beginning to explore the internet that your child realises that other internet users may not be who they say they are and that 'friends' made online are still strangers, so personal information should be kept safe, including their name, address, phone numbers and passwords etc. Encourage the use of screen names and nicknames where possible. This is where a **family agreement** can be incredibly useful, to establish rules and good online behaviour in advance.





What games are okay for my child to play?

There are many different online games and playing experiences currently available to children e.g. via computers, consoles, internet games and apps. Gaming may be the very first way that your child encounters life online. Some games however are for adults or older audiences and contain images and language that are not suitable for children. Therefore it is important that the games your children play are the correct age rating. Like film classifications, these ratings are determined by the game's content, and all video games sold in the UK are clearly marked with age ratings set by PEGI (Pan European Games Information). Google Play and Windows Store apps are also rated by PEGI.

Many games allow children to play with other internet users and may have chat features enabled. Some games provide a "safe chat mode" where simple predetermined phrases can be used. Playing these games yourself can be fun and will also enable you to identify the safety features provided, such as reporting to a moderator. Reading online reviews of games can be a really useful way to hear other parents' experiences and feedback, and highlight potential safety issues like whether 'in-app' adverts are present, and whether the adverts displayed are suitable for the audience for which the app is intended. There have been news stories of young children running up large bills by inadvertently making 'in-app' purchases whilst playing, so do look out for whether you can spend real money during the game; it should be in the app description in the app store. You can also disable 'in-app' purchasing on a number of devices within the settings.

Where can I report?

Reports can be made to websites through safety/help centres and moderation services. If you are suspicious about the behaviour of others online, reports can be made to CEOP and inappropriate media content, online and offline can be reported via Parentport. Criminal content online can also be reported to the IWF. For more information regarding reporting, visit our Need Help? section on the Childnet website.





Useful Links:

www.childnet.com/parents-and-carers/need-help www.childnet.com/have-a-conversation www.saferinternet.org.uk/parent-tech www.saferinternet.org.uk/parental-controls www.ceop.police.uk www.parentport.org.uk www.iwf.org.uk www.pegi.info







This guide has been written and produced by children's charity Childnet International as part of the UK Safer Internet Centre. Copyright © 2016. Registered Charity no. 1080173.



KEEPING YOUNG CHILDREN SAFE ONLINE

Children love using technology and are learning to navigate websites, online games and consoles, and touch screen technology like iPads and smartphones from a younger and younger age.



Latest Ofcom research has shown that 91% of 5-15 year olds live in a household with internet access and over a third of all 3-4 year olds are now accessing the internet in their homes. We know that children need support in these environments, to get the best out of using the internet, and there are real advantages in making sure that children are supported in their internet use right from the start.



These eight frequently asked questions will provide you with useful information and tips that you can put into place at home, to help keep your youngest children safe online.



Where do I start?

The best way to keep your family safe online, and to understand your children's internet use, is to use the internet together. Active engagement and conversations with your children are key. Be positive and embrace the technologies that young children enjoy and look for family activities or games. Take time to explore the games and services that your children are using, or want to use, and look out for any safety features that may be available. This will give you a better understanding of the different ways that children are engaging with technology and help you to feel more confident.

Should I set any rules?

In the same way that you set rules for most areas of your children's lives, establish your expectations regarding online activities. Creating a family agreement is a useful step, which might include time spent online, sites that can be visited, and behaviour expected; remember, what's right and wrong offline is also right and wrong online. It's a great idea to agree these rules from the outset, so that you and your children are aware of their boundaries.





How can I supervise my child?

Placing your computer or laptop in a busy part of the house e.g. the living room or kitchen can be helpful. This can make it easier for you to be involved in their technology use. But remember, the internet can be accessed from a number of portable devices, for example smartphones, iPod Touch, games consoles and tablets. Portable devices may allow you to ensure your children are using them where you can see them and your children can still be supervised. To find out more about the internet capabilities of smartphones, gaming consoles and other devices, check out our Parents' Guide to Technology.

How much time is too much time?

Children can be enthusiastic users of technology. The challenge can be to harness this enthusiasm and ensure a balance, so that the use of technology does not negatively impact on other important areas of young children's lives. There are some strategies that can be used to help manage the time online issue, such as agreeing time limits or using time limiting tools, designating weekly times to use the internet together, or removing portable devices from your child's bedroom at night to avoid tiredness.





Are there tools to help?

There are free parental controls and filters available, to help you set safer boundaries for your children, but you will usually be required to set them up. Your internet service provider (such as BT or TalkTalk) will provide free filters to help block age inappropriate content for children, and on the UK Safer Internet Centre website you can watch video tutorials that show you how to find and set these up. All mobile phone operators (such as O2 or Vodafone) also provide such parental controls for free. The websites of device manufacturers (such as games consoles) should also outline the controls to which you have access.

Filtering options can be found within websites and services themselves, for example on YouTube or 'safe search' settings can be applied to search engines such as Google or Bing. There are even some search services designed for children (such as Yahoo! Kids). Parental controls can be password protected, so it's advisable to choose a strong password and not share it. Parental controls and filters are a good starting point but it is important to recognise that they are not 100% effective. They are a great help, but not a solution, and work best in combination with parental supervision and engagement, to help your children understand how to stay safe online. As children grow and develop, so do their online needs, therefore you may want to periodically review your parental controls to accommodate this.

What advice can I give my child?

Education is the best tool that a child can have, so discuss with your child the importance of telling an adult immediately if someone, or something, upsets them online. Make sure that your children know that they can come and talk to you (without necessarily getting into trouble) if they see anything that worries them on the internet, and encourage them to feel confident enough to do so. Other immediate strategies to deal with unwanted content or contact could include; switch the screen off, close the laptop, exit the website, or turn the iPad or phone over and put it down.

Younger users may be distracted by advertising and pop ups and with just a couple of clicks, or a spelling mistake, may find themselves on a different website. Children are naturally curious and will innately push boundaries. Bookmarking sites or creating a 'favourites' list is a simple way to help your children find the content they want without having to search the internet for it. It is also important whilst beginning to explore the internet that your child realises that other internet users may not be who they say they are and that 'friends' made online are still strangers, so personal information should be kept safe, including their name, address, phone numbers and passwords etc. Encourage the use of screen names and nicknames where possible. This is where a family agreement can be incredibly useful, to establish rules and good online behaviour in advance.





What games are okay for my child to play?

There are many different online games and playing experiences currently available to children e.g. via computers, consoles, internet games and apps. Gaming may be the very first way that your child encounters life online. Some games however are for adults or older audiences and contain images and language that are not suitable for children. Therefore it is important that the games your children play are the correct age rating. Like film classifications, these ratings are determined by the game's content, and all video games sold in the UK are clearly marked with age ratings set by PEGI (Pan European Games Information). Some online games may also be age rated or be classified 'PEGI OK.'

Many games allow children to play with other internet users and may have chat features enabled. Some games provide a "safe chat mode" where simple predetermined phrases can be used. Playing these games yourself can be fun and will also enable you to identify the safety features provided, such as reporting to a moderator. Reading online reviews of games can be a really useful way to hear other parents' experiences and feedback, and highlight potential safety issues like whether 'in-app' adverts are present, and whether the adverts displayed are suitable for the audience for which the app is intended. There have been news stories of young children running up large bills by inadvertently making 'in-app' purchases whilst playing, so do look out for whether you can spend real money during the game; it should be in the app description in the app store. You can also disable 'in-app' purchasing on a number of devices within the settings.

Where can I report?

Reports can be made to websites through safety/help centres and moderation services. If you are suspicious about the behaviour of others online, reports can be made to CEOP and inappropriate media content, online and offline can be reported via Parentport. Criminal content online can also be reported to the IWF. For more information regarding reporting, visit our Need Help? section on the Childnet website.





Useful Links:

www.childnet.com/parents-and-carers/need-help www.saferinternet.org.uk/parent-tech www.saferinternet.org.uk/parental-controls www.ceop.police.uk www.parentport.org.uk www.iwf.org.uk www.pegi.info













1: Online gaming, an introduction

Online gaming is hugely popular with children and young people. Recent research shows that gaming is one of the top activities enjoyed by 9-16 year olds online, with gaming more popular than social networking.

From sport related games to mission based games and quests inspiring users to complete challenges, interactive games cater for a wide range of interests, and can enable users to link up and play together.

Games can provide a fun and social form of entertainment often encouraging teamwork and cooperation when played with others.

Just like offline games, they can have educational benefits, and be used, for example, to develop skills and understanding.

Traditionally, games could be bought from shops, often in the form of a disk for use on a PC or console. Now, games can also be downloaded online. Games are played on many platforms, with those bought in shops often having an online component to them.

Internet connectivity in a game adds a new opportunity for gamers as it allows players to find and play against, or with, other players from around the world (in a multi-player game).

We know that parents and carers do have questions and concerns about games, often about the type of games their child plays, and for how much time their child is playing.

This leaflet provides an introduction to online gaming and advice for parents specifically related to online gaming.



2: Online gaming, where and how?

There are many ways for users to play games online. This includes free games found on the internet, games on mobile phones and handheld consoles, as well as downloadable and boxed games on PCs and consoles such as the PlayStation, Nintendo Wii or Xbox.

Some of the most common devices on which online games are played are listed below.



Consoles: These games are played on home entertainment consoles designed to work with a TV. Games for consoles are mostly boxed products bought in shops and also online, containing a game disc

and usually a manual. According to Ofcom, nearly three quarters of children aged eight and over, have a games console, in their bedroom. Consoles like these are capable of connecting to the internet via a home network just like other computers. This allows users to download games or 'expansions' to existing games as well as playing online, although a subscription may be required for this. All of the three main manufacturers (Nintendo, Sony and Microsoft) include parental control functions in their consoles that are linked to age ratings systems (FAQ 2).



PC Games: These games are played on a personal computer the same way as other software programmes. They can be bought from shops or purchased and downloaded directly from the internet.

Many PC games make use of the internet, and many 'Massively Multiplayer Online' (MMO) games, where gamers interact together in virtual spaces, are PC games.



Web Games and Applications (apps): Some games are accessed through a unique website, and there are also websites hosting hundreds of different games. Many of these games are free of charge online,

although some may have paid-for components. Applications can be accessed through, and downloaded to, social networking profiles which allow users to play games on their profile as well as enabling them to play games with their friends, generally for free. Smart phones with internet connectivity also enable users to download games to play, some free, some charged for. In contrast to console and PC games, many web games and downloadable app games are not rated.



Mobile Games: Mobile games can be free or chargeable. There may be costs associated with mobile gaming, as within some games, even free ones, there are opportunities to purchase added functionality

such as 'in-app' purchases. These functions however can be deactivated, usually through the phone settings.



Handheld Games: Handheld games are played on small consoles. Two of the current popular handheld consoles are the Nintendo DSi and the Sony Playstation Portable (PSP). Handheld games can also be played on

other devices like the iPod Touch or iPad. These devices can also access the internet wirelessly, and allow for playing games with others online.

3: Online gaming, the risks

Internet safety advice is directly applicable to the games environment because risks of **Content**, **Contact**, **Conduct** and **Commercialism** also apply to games.

Content: inappropriate material is available to children online.

The quality of graphics in many games is very high. Some games might not be suitable for your child's age – they might contain violent or sexually-explicit content.

Contact: potential contact from someone online who may wish to bully or abuse them.

If your child takes part in multi-player games on the internet (where they play against other people, potentially from all around the world) they might be at risk of hearing offensive language from other players, being bullied, or making themselves vulnerable to contact by those with a sexual interest in children if they give out their personal details. Bullying on games is known as 'griefing'. This is when players single out others specifically to make their gaming experience less enjoyable.

Conduct: children may be at risk because of their own and others' online behaviour, such as the personal information they make public.

Specific conduct risks for gamers include excessive use to the detriment of other aspects of their lives. This is sometimes referred to as 'addiction'. Some websites might not have the game owner's permission to offer a game as a download i.e. copyright infringement, the same as for music and film, and by downloading it the user might be breaking the law.

Commercialism: young people's privacy can be invaded by aggressive advertising and marketing schemes.

Children and young people can get themselves into difficulty by inadvertently running up bills when playing games online. Some online games, advergames, are designed to promote particular products.



- » It may seem daunting, but one of the best things parents and carers can do is to engage with the gaming environment and begin to understand what makes it is so attractive to young people as well as the types of activities that they enjoy!
- » Talk with your children about the types of game(s) they are playing. Are they role-playing games, sports games, strategy games or first person shooters? If you're not sure what they are, ask them to show you how they play and have a go yourself.
- » Some games may offer children the chance to chat with other players by voice and text. Ask them who they are playing with and find out if they are talking to other players. If chat is available, look at the type of language that is used by other players.
- » Remember that the same safety rules for surfing the net apply to playing games on the internet. Familiarise yourself with the SMART rules, and encourage your children and young people to as well

5: SMART rules

Safe: Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your e-mail address, phone number and password.

Meeting: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

A Accepting: Accepting e-mails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

Reliable: Someone online might lie about who they are and information on the internet may not be true. Always check information with other websites, books or someone who knows. If you like chatting online it's best to only chat to your real world friends and family.

Tell: Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

6: Online gaming, frequently asked questions

1: What are the ways in which my child might be communicating via online video games? What tools are available to help my children here?

Many games offer users the ability to chat with other gamers during the game. Players can 'talk' by using Instant Messenger type messages typed in the course of the game and also by voice conversation (made possible through headsets) which is similar to talking on the phone.

Parental control tools are provided on PCs and consoles, and these can limit gameplay functionality, including chat. Make sure your children know how to protect their privacy. Advise them never to give out any personal information, pictures of themselves, or agree to meet someone in person, when using online chats or sharing information in their user profile.

Make sure they know how to make the most of privacy features built into gaming, internet and mobile services. These could include using a voice mask to disguise their voice in a multi-player game as well as how to block and report other players and use the mute function which can disable chat in many games.

Encourage your child to use an appropriate screen or character name (also called gamertags) that follow the rules of the game site. These names should not reveal any personal information or potentially invite harassment.

In addition to chatting within a game, many gamers chat on community forums and content sites related to the games they are playing. Gamers use these sites to exchange information about the games as well as to provide tips and hints to others. It is important to encourage your child to remember to respect their privacy on these sites too and locate the means for reporting any issues they encounter.

2: How do I know which game is appropriate/ suitable for my child?

The Pan European Game Information (PEGI) age rating system exists to help parents make informed decisions on buying computer games, similar to the BBFC ratings for films. The rating on a game confirms that it is suitable for players over a certain age, but is not indicative of the level of difficulty.

PEGI age labels appear on the front and back of games packaging. Additional 'descriptors' shown on the back of the packaging indicate the main reasons why a game has received a particular age rating. Parents should particularly be aware of the 'online gameplay' descriptor which indicates whether a game can be played online. With online games, use of this descriptor indicates that the game or site is under the control of an operator who has signed up to the PEGI rating system.

Encourage your child to only access online games that are appropriate for their age and always check the age rating on any game before buying it for your child, as well as considering whether it has an online component.













3: Are there parental controls that I can apply?

There are parental controls that you can set based on your child's age and maturity, so make the most of parental controls and privacy features provided by games, console, internet and mobile companies to help protect young gamers. However, these controls aren't a substitute for parental involvement.

4: How can I report inappropriate behaviour by another user?

Sadly cyberbullying by 'griefers' can occur in online games. If your children are being harassed by another player on a game, follow the game's grief-reporting guide to report this behaviour. Inappropriate behaviour can also be reported to the moderator on a moderated game and in many instances you can contact the customer support team for further assistance. If your child does encounter inappropriate behaviour in an online game, encourage them to block that user. If you are suspicious of the behaviour of another user towards a child, you can report them to the police at www.ceop.police.uk.

5: How long should I let my child play online games for?

Consider what is appropriate for the users in your house and their gaming needs. This may depend on the type of game they are playing, as quest based games for example are unlikely to be completed within ½ hour. Agree together rules of playing games online, which as well as covering safety considerations could include play time limits. You may find it more appropriate to set a weekly quota for their internet use or to agree that certain games should only be played at a weekend. UKIE, the body that represents the interactive entertainment industry in the UK recommends that all games should form part of a healthy and balanced lifestyle and as a guide games players should take five minute breaks every 45 - 60 minutes.

6: What else should I consider?

As well as staying safe when playing online games, it's also important to stay legal. It may be tempting to download cheat programmes to skip to a higher level, but these, and downloading uncopyrighted games, can expose users to unsuitable content and viruses affecting your computer.



争 7: Online gaming, support and more information

Childnet's **Chatdanger** site, **www.chatdanger.com** offers guidance about chatting on the internet.

Video games trade body **UKIE** offers advice about how to play games safely and sensibly from the 'playsafe' area of their website www.ukie.info/playsafe.

Visit the **Pan European Game Information** and **Entertainment** Software Rating Board websites www.pegi.info/en/ to find out more about age ratings.

Check out the websites of the games companies such as **Microsoft**, **Nintendo** and **Sony** to look at the parental support







Online Reputation Checklist

Your digital footprint is the mark that you leave behind when using the internet and can shape your online reputation. Your digital footprints can be positive or negative and can influence how people see you now or in the future. Use our simple checklist to help manage and maintain your online reputation.



Make a positive footprint

The internet is a fantastic way to shout about all your achievements and to let everyone know about all the amazing things you create and do online. The best way to keep your online reputation in check is to use your time online to get creative and leave a positive mark behind. For example, you could write a blog to promote all the great things you're doing or create a video to teach others something new.



Search yourself online

Do you know what is online about you? It's recommended that you search your name online regularly. You might be aware of the content you post about yourself online, but are you aware of what others post about you? Set up Google Alerts - where you will receive an email every time your name appears in a Google Search result. Remember: if your Instagram or Twitter pages appear you can change this by adjusting your privacy settings.



Check your privacy settings

Make sure you know what information you are sharing on the platforms you use, in particular social networking sites. Most social networking sites have privacy settings to help you manage the content you share and who you share it with; you can decide if you want your posts to be shared with all your online followers, or a specific list of followers or the public. Keep in mind that your friend's content and their settings can also affect your digital footprint; remember you're only as private as your most public friend! Have a look at www.saferinternet.org.uk/safety-tools to learn about how to set up privacy settings on



Think before you post

Be proud of everything you post online! Before you post that silly photo of a friend on Instagram, ask yourself if you would be happy for that same friend to post a photo like that of you. Even if a service states that once you post a photo it will disappear after a certain period of time, once something is online it could potentially be there forever!



Deactivate and delete

If you stop using a social media account it's a good idea to deactivate or delete your account. Deactivating your account means that you can still access the content posted for a period of time. Deleting the account removes the account completely. Over time, this will prevent it appearing in search results on a site or through a search engine, and it will remove the risk of these accounts being hacked without you knowing.







so you got naked online.

A resource provided by the South West Grid for Learning







So you got naked online...

OK... so I guess if you have picked this up and started to read, it's likely that you have done something online that you are now regretting. Or perhaps you are trying to help someone who has done something? And if that something involved nakedness or something sexual, then that may look more serious than other things you see happening online.

But don't freak out just yet... you are obviously keen to find out more about how you can help yourself or your friend and perhaps get some advice and a plan for how to improve things. Well, you're in the right place.

Read on and you will discover:

- Why these things happen and what different people think about it.
- When it has happened to **others** and what they have done.
- How the technology works and what the possible risks are.
- What the first things are you can do to begin to take control.
- Whether your fears of getting into trouble are realistic.
- The impact on you for the future and what you can do about it.
- How to get support and advice from organisations who are there to help vou for just this sort of issue.

Contents:

P2: Introduction

P3-4: Amanda Todd's Story
P5: What does it mean?

P6: Deliberate or accidental

P7: Sharing pictures

P8-10: All about trust

P11: Where might your picture be?

P12: What should I do first?

P13: Who can help me?

P14: Knowing about reputation

P15: Organisations that can help

p16: About this resource

However, this isn't helping yet, so let's crack on. You don't have to read this whole thing through but it does help to browse each section to get a really good understanding of how and why this stuff causes problems. The more clued-up you are, the better decisions you are going to make for yourself (or friend).

"Knowledge is power"

Amαndα's story... Amanda Todd committed suicide at the

age of 15 at her home in British Columbia, Canada. Prior to her death, Amanda posted a video on YouTube in which she used a series of flash cards to tell her experience of being blackmailed into exposing her breasts via webcam, being bullied and physically assaulted. The video went viral after her death resulting in international media attention. As of April 2014, the video has had more than 17 million views... Her mother Carol Todd has since dedicated her time to awareness raising on the issues which affected Amanda, and supports the work of the Safer Internet Centre.

Below Carol has some advice for any young people affected by sexting.

Amanda Michelle Todd

(November 27th 1996 - October 10th, 2012)

My daughter, Amanda Michelle Todd, took her life at the age of 15. It all started with a topless photo. She didn't know the person at the other end of her computer was taking a picture. She didn't know that he was showing it to other men. Then she started to get blackmailed into showing more of herself via her webcam. And if she didn't, then her image would be sent throughout the internet. What Amanda didn't do was tell an adult that this was happening to her. She kept it to herself. This image and what happened thereafter was the start to the emotional



breakdown of Amanda. The loss of her confidence, her spirit and her friends. The embarrassment that followed was unbearable as was the name-calling, the slutshaming and the bullying online and offline that occurred. Eventually Amanda retreated into a shell, not being able to re-emerge as the girl she once was.

As a parent and Amanda's mother, it is important to me that young people understand what can happen online and also how to protect themselves online. 'So you got naked online' is a resource guide that was developed in the U.K. but will still have impact with its clear messages anywhere in the world, even in Canada where Amanda lived. The issues and concerns related to technology use among young people remain the same everywhere. It doesn't really matter where in the world we live.

As an educator and a parent, this guide is written in 'youth friendly language' that both encourages and acknowledges a young person to be responsible if they have done something regrettable online (eg – sexting, sending images out). It also reiterates how challenging the internet can be these days by how quickly images, words and files can be shared and where items are stored with and without our knowledge. Our young people need to know that and this is a perfect platform to share it.

We need to always tell our young people that it is okay to admit to making a mistake and then also to support them in talking to an adult. This action is so very important before things escalate. We all need to remember that making mistakes is normal and a part of growing up. The teen years is when a lot of these happen. Also that these experiences becoming learning experiences for the future years.

I applaud those that participated in the writing and development of this guide. It conveys the right messages in a way that is easily read and understood. I hope that it is read by all young people and their parents and goes beyond the school into the communities and cities we live in.

Sincerely, Carol Todd (Amanda's Mom)

For more information on Amanda's story, please visit:

http://amandatoddlegacy.org



I see sexting mentioned in the newspapers. What does it mean?

"Teen sexting is a very rational act with very irrational consequences." danah boyd

"Sexting" is a term used to describe the sharing of intimate images or video with another person.

This content can be anything from texts, partial nudity right up to sexual images or video. Very often it is between partners, but can be between groups and can use a whole range of devices, technologies and online spaces. The most common ones are by **text**, **private message** on social networks or **apps** such as **Kik**, **Oovoo**, **Instagram** or **Skype**.



Deliberate and Accidental

Most sexting is deliberate; the person sending the content means it to happen. They will pose or act in a sexual way and will make a direct effort to send it to the person they want to see it, usually a boyfriend or a girlfriend.

Occasionally, if you have personal pictures of yourself on your phone it might be possible to accidentally "share" it via email, text or Bluetooth

with the wrong person but this is unusual. There have also been cases where pictures have been spread after mobile phones have been stolen. Accidental sexting is more likely to happen if your judgement is clouded e.g. if you have had alcohol or taken drugs or are under pressure from those around you. This could result in you:



- getting confused and pressing the wrong send button
- feeling brave about risking a naughty photograph
- · feeling more sexually confident
- feeling less inhibited, less aware of risk and the consequences
- being encouraged by mates to do it as a dare
- thinking that it is a good laugh and there is no harm in it

The accidental stuff happens once it has left your control, but more about this later.

Both Deliberate and Accidental?

Some people think it's cool to copy what they see in the media but celebrities also get caught out! Despite the concerns, sexting has become a part of modern life. We see references in popular culture such as the 2014 "comedy" film Sex Tape starring Cameron Diaz, or the song "Dirty Picture" by Taio Cruz and Kesha which reached no.6 in the UK charts.

The media has been full of stories of leaked personal photos of celebrities such as the iCloud incident where actresses including Jennifer Lawrence and Kirsten Dunst had their images hacked and posted onto 4chan, or the "Snappening",

where a third party app was hacked which was hosting thousands of Snapchat images. **Many of these were then re-posted onto sites such as Facebook and Tumblr and were of teenagers, technically indecent images of a minor.**



LOL or OMG?!

People sharing naked pictures as part of a safe relationship is not a new thing.

What has changed though is the speed with which you can share. Using webcams or sending mobile pictures can be a spontaneous decision, made without thinking about what could happen and what people might think. Once the picture leaves your control it can easily and quickly be shared with many people.

A study by the Internet Watch Foundation showed that up to 88% of self-generated images have been collected and put onto other sites!



In your parents' younger years, the embarrassing stuff they did was rarely seen by anyone else. Today with mobile phones and the web that has changed. The World Wide Web means the potential of a huge audience and of course, if a photo is uploaded and shared, it can be on there forever. Pretty scary thought that something stupid you do at 14 can still potentially affect your adult life.

This is not the end of the world. It just needs some thought on how you can minimise the effect of your mistake.

Was I right to have trusted the person I sent it to? Was I being naive?

Most of the time, these intimate pictures are shared between boyfriend and girlfriend, and let's be honest, you wouldn't send them if you didn't trust the other person would you? There are probably many images shared which never leave the intended recipient, even when the relationship ends. **So ask yourself, if we break up, will this person respect me enough not to share my pictures?** How well do you really know them? Sadly, it is often only when we split up with someone that we see their true colours.

Sometimes yes you can trust the person you text.

But, and this is a big but, do you really need to send them pictures of your body? If the person asking for this acts up when you refuse, is this someone you can trust? If they accept your refusal without question they sound like a good partner.

Others letting you down...

Some of the problem will be around people you thought you could trust, sharing the image or joining in the negative comments. This might be the person who you sent the image to in the first place, or mates or others who then circulate it. People get caught up in gossip, banter or bitching sessions, often without meaning harm to the victim, either to impress other people, to "belong", or because it starts as a joke which escalates. Sometimes people do it to bully someone.

What if other people see it?

There is a big difference between worrying and understanding how far the image may have gone beyond your control.

It depends how the image was published; if you sent it directly to someone's mobile and then had second thoughts, you need to have an honest conversation with them as soon as possible to get them to delete it.





Posting directly to social networks makes it harder to regain that control. Modern social networks and apps are designed to make publishing and sharing quick; the software makes those connections for you... and that's the trouble. It's hard to know where the image has gone and who has got it. It can very quickly leave your social circle and spread to others.

But there are ways in which you can challenge content about you that has been published by others using the site's **"report abuse"** option. It's important to draw their attention to it and why you think it should be removed. It's not enough to say "I don't like it"; your request needs to show that it breaks their terms and conditions of use. **Sites like Facebook and Instagram don't allow nudity so it should be easier to report. We've included some links to these reporting routes at the end of this booklet.**

It is also important to understand how you yourself can change or remove content that you have posted about which you have changed your mind. That profile pic of you in your underwear was funny at the time but ...

It's important in life to have friends around you that you can trust and on whom you can rely; this is no different online. It's less likely your close friends would want to do anything serious to hurt you; very often they're the first ones you might turn to for help.

I REALLY NEED A FRIEND RIGHT NOW!

Use those friends you can trust to help put out the messages we want and recover the situation where they can.

That's why it is important to think carefully about your social network friends lists and ask yourself "Who would stand beside me when things go wrong?"

What is your definition of a "friend" or a "friend of a friend"? We often add friends because our other friends know them. In reality the person may have been passed on through lots of lists like this. If they have, then this makes it more difficult to track who has seen a naked picture you may have posted, as it has spread across groups you don't belong to. It may even be public which could mean literally anyone on the internet could see it.

There are ways in which you can choose who sees what on your profile (privacy settings) and this might be something you would want to get up Here's a link to a "down and dirty" guide to how you can take control of your privacy on Facebook www.swgfl.org.uk/FacebookChecklist















Where your picture might be:

Peer to peer sites - sharing files is a worldwide system used by all kinds of people. Images are exchanged in bulk and can become part of collections in folders that very often sit on other people's computers. This means adults and others you don't know viewing your personal naked pictures on the likes of Piratebay and Demonoid sites.



Photo sharing sites like Flickr or Instagram allow open and unrestricted (as well as private) sharing of pictures.

Your data could be on company's servers or copied to users' personal devices.



Webcam sharing sites can also cause problems when people record your actions. Sites like Omegle and Chat Roulette often attract criminal elements.

Sometimes these "anonymous" services encourage people to be more adventurous and risky, but being online is never completely anonymous. It only takes screen or webcam capture software to end up with a video clip.



Online Groups and Communities also often contain sex offenders who will form close knit groups and share indecent images (many of which they will obtain from the web).



Cloud storage sites like iCloud, OneDrive, GoogleDrive, or Dropbox allow server space for people to store material such as images. Other users with permission can then access the files.

Once again it is difficult to know where your content actually sits and where the cloud servers are based. Those that are based outside of the UK or European Union often don't have the same strict laws about personal data that we have and your content could be sold and shared with other networks across the world.

What are the first things I should do?

It might seem like the end of the world but try not to panic! Take a deep breath and give yourself a chance to think about how this might affect you.

First off, are you OK? Do you need support? If you do, find the best person to support you right now... friends, family, school? You choose. **There is also a list of organisations at the end of this booklet that can help.**

Sometimes that first step of asking for help is a difficult one. But you have to be honest with yourself. Real friends and professionals trying to help are only able to do so when they know all the facts and how you feel about it. If you know of a friend who is trying to deal with this maybe you could show them this!



If you decide you need to do something, don't wait. The quicker you deal with it the better chance there is of managing the spread.

Will I get into trouble?

The Law is on your side and was not designed to punish young people for making mistakes whilst experimenting with their sexuality.

The law is aimed firmly at those who choose to trade or profit from sexual pictures of children.

Even though (if you are under 18) the image(s) you have sent may constitute an indecent image of a child, the Association of Chief Police Officers have clearly stated that young people will be treated as victims in the first instance and only extreme cases may be reviewed or looked at differently. They clearly state "First time offenders should not usually face prosecution for such activities, instead an investigation to ensure that the young person is not at any risk and the use of established education programmes should be utilised".

Who can help me?

Parents

It may be your worst nightmare thinking of telling your parents you shared intimate pictures, and yes, they may kick off at first but they need to know; how are they going to support you if they don't know?

Use your discretion, if you don't think the pictures will go viral, then don't upset them for no reason. If you feel there is a risk, or if your picture has already been shared, then you need them on board. Yes, they will probably be very upset and disappointed, but they'll get over it! **And will probably respect you more for being upfront about it...**

School

You might want to consider telling someone at school. It might seem like a hard thing to do but your welfare is their number one concern. Trained staff will have access to a whole range of help that will be much more effective than dealing with it on your own. One service they can use is the Professionals Online Safety Helpline www.saferinternet.org.uk/helpline

CEOP

CEOP is the Child Exploitation Online Protection centre and was set up by the Government in 2006 to help protect children online across the **UK from online predators.** As well as helping UK police forces to bring these people to justice, CEOP can help provide advice to you and your parents when something like this happens. You can report at

http://bit.ly/p8kAKF or by going to the CEOP website at www.ceop.police.uk. There is also a great film about Sexting called 'Exposed', it's on Youtube at http://bit.ly/hePkDE.

Local Police

Police could possibly be involved if it involves the well-being of other pupils, and could also offer effective support.



Is this going to affect things for me in the future?

Hopefully in most cases your continuing digital life will 'bury' your mistakes as time goes on. There is however no guarantee that the pictures will not be seen by others later. Your reputation could be affected if future employers, college, or sixthform friends see this. Being honest and open and admitting a mistake is the best approach, as it will be with any future relationships.

Knowing about reputation

Do you know what's online about you?

You should first check what others can see about you. Search for your name using Google or other search engines and see what information already exists about you. Although you may not have added anything new, your friends and family might have.

If you find anything offensive or require anything removed, report it to the hosting site immediately. Remember it will need to break the site's terms and conditions. If it is a naked or semi-naked image of you it is highly likely to breach these conditions and the legal implications mean the site host is likely to remove it quickly when made aware.

Bury the bad stuff! Increasing your positive online presence... Sadly there are some occasions where online content can't be removed, for example if your image is shared via an adult site hosted outside the UK we advise that you try and bury the content you don't want people to see. The best ways to do this are to set up social networking accounts, (you don't have to use them, just set them up and leave your name publicly searchable), to regularly comment on news articles and forums, and also to run a small blog. The more you add the further down the search lists this unwanted content will be.

Show me organisations that might be able to help me:

There are lots of places you can go to for help and advice, consider who is the best person to support you. It could be a Youth Club, Employment Advisor, Faith Leader, or Sports Coach. Anyone who is trained to support young people should have an idea what to do to help you.

Our partners at the Internet Watch Foundation and Childline are working together to help you remove sexting images. They won't judge you: they'll just help you. Get in touch at www.iwf.org.uk

There are also many national organisations who can help such as:

Childline www.childline.org.uk

Get Connected www.getconnected.org.uk

ThinkUknow www.thinkuknow.co.uk

Or download the Zipit app from the Childline website (Supported by IWF)

Be prepared to explain:

As a final note, you should be prepared to explain the following things..



- I've made a mistake
- I've been really stupid
- I have learnt by it
- I have moved on

About this resource:

This is a resource for children, young people and parents that offers advice and explores strategies to support the issues resulting from sexting incidents.

The resource will be available shortly in the following alternative formats:

- A printed resource
- A comic book style summary of key advice for young people
- Interactive web resource from the UK Safer Internet Centre

Visit **www.swgfl.org.uk/sextinghelp** for more information.

It is produced by the South West Grid for Learning and UK Safer Internet Centre and co-funded by the European Union.







The South West Grid for Learning Trust is a not for profit, charitable trust company, providing schools and many other educational establishments throughout the region with safe, secure and reliable broadband internet connectivity; broadband-enabled learning resources and services and help, support and advice in using the internet safely. Find more resources at www.swgfl.org.uk.

department for children, schools and families

Cyberbullying

A whole-school community issue

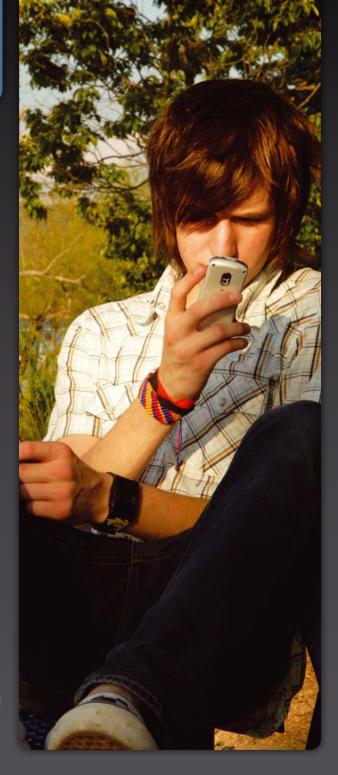
Introduction

Today's children and young people have grown up in a world that is very different from that of most adults. Many young people experience the internet and mobile phones as a positive, productive and creative part of their activities and development of their identities; always on and always there. Above all, information communication technologies support social activity that allows young people to feel connected to their peers.

Unfortunately, technologies are also being used negatively. When children are the target of bullying via mobile phones or the internet, they can feel alone and very misunderstood. They may not be able to identify that what is happening to them is a form of bullying, or be confident that the adults around them will understand it that way either. Previously safe and enjoyable environments and activities can become threatening and a source of anxiety.

As mobile phone and internet use become increasingly common, so has the misuse of this technology to bully. Current research in this area indicates that cyberbullying is a feature of many young people's lives. One study carried out for the Anti-Bullying Alliance found that 22% of young people reported being the target of cyberbullying.

This document explains how cyberbullying is different from other forms of bullying, how to respond and combat misuse through a shared responsibility, and how to promote and develop a culture of confident technology users to support innovation, e-safety and digital literacy skills.



'Cyberbullying, A whole-school community issue' is a summary of the Department for Children, Schools and Families (DCSF) Guidance for schools on preventing and responding to cyberbullying, which was written in conjunction with Childnet International and published in September 2007. This document seeks to give practical advice to young people, their carers and school staff about the issue of cyberbullying.



What is Cyberbullying?

Cyberbullying is the use of Information Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else.

What's different about cyberbullying?

Bullying is not new, but some features of cyberbullying are different from other forms of bullying:

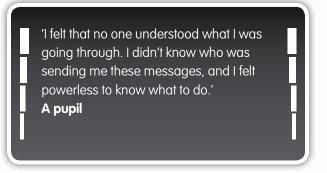
- 24/7 and the invasion of home/ personal space. Cyberbullying can take place at any time and can intrude into spaces that have previously been regarded as safe or personal.
- 2. The audience can be very large and reached rapidly. The difficulty in controlling electronically circulated messages means the scale and scope of cyberbullying can be greater than for other forms of bullying. Electronically forwarded content is hard to control, and the worry of content resurfacing can make it difficult for targets to move on.
- People who cyberbully may attempt to remain anonymous. This can be extremely distressing for those being bullied. The person cyberbullying may never be in the same physical space as their target.
- 4. The profile of the bully and target. Cyberbullying can take place both between peers and across generations; teachers have also been targets. Age or size are not important. Bystanders can also become accessories to the bullying; for example, by passing on a humiliating image.
- 5. Some instances of cyberbullying are known to be unintentional. It can be the result of not thinking (something sent as a joke may be deeply upsetting or offensive to the recipient) or a lack of awareness of the consequences for example saying something negative online about another pupil, or friend that they don't expect to be forwarded or viewed outside their immediate group.
- 6. Many cyberbullying incidents can themselves act as evidence. This is one of the reasons why it's important to know how to respond!

Cyberbullying and the law.

Education law: Bullying is never acceptable. The school community has a duty to protect all its members and provide a safe, healthy environment. A range of Education Acts and government initiatives highlight these obligations.

The Education and Inspections Act 2006 (EIA 2006) outlines some legal powers which relate more directly to cyberbullying. Head teachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off site. The EIA also provides a defence for school staff in confiscating items such as mobile phones from pupils.

Civil and criminal law: Although bullying is not a specific criminal offence in UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications. In fact, some cyberbullying activities could be criminal offences under a range of different laws, including the Protection from Harassment Act 1997, which has both criminal and civil provision, the Malicious Communications Act 1988, section 127 of the Communications Act 2003, and the Public Order Act 1986.





Preventing Cyberbullying

The best way to deal with cyberbullying is to prevent it happening in the first place. The key first step is deciding who within the school community will take responsibility for the coordination and implementation of cyberbullying prevention and response strategies. It's best if this person is a member of the school's senior management team and/or the staff member responsible for coordinating overall anti-bullying activity. This person will need to have experience of making sure the whole school community contribute to, and are included in, activities.

There is no single solution to the problem of cyberbullying. These are the five key areas schools need to address together to put in place a comprehensive and effective prevention plan:

1. Understanding and talking about cyberbullying

The whole school community needs a shared, agreed definition of cyberbullying. Everyone needs to be aware of the impact of cyberbullying and the ways in which it differs from other forms of bullying. Young people and their parents should be made aware of pupils' responsibilities in their use of ICT, and what the sanctions are for misuse. Students and parents should know that the school can provide them with support if cyberbullying takes place out of school.

2. Updating existing policies and practices

Review and update the school's anti-bullying policy plus other relevant policies – for example, policies on behaviour, pastoral care and e-learning strategies. Review your existing Acceptable Use Policies (AUPs) – the rules that students have to agree to follow in order to use ICT in school – and publicise them to parents and students. Keep good records of any incidents of cyberbullying. Be able to conduct searches of internet use records at school. Knowing that the school is taking such steps may act as a disincentive for bullies to misuse school equipment and systems.

'Having my daughter show me text messages from nearly everyone in her class, all saying derogatory things about her, was devastating.'

A parent

3. Making reporting cyberbullying easier

No one should feel that they have to deal with cyberbullying alone, but reporting any incident of bullying can be really hard for the person being bullied and for bystanders. Provide and publicise different ways of reporting cyberbullying in schools – for instance, a student council taskforce, peer reporting, anonymous reporting – and provide information about contacting service providers directly.

4. Promoting the positive use of technology

Technology is successfully being used to support engaging, positive and effective learning, and to realise and increase the potential of personalised learning by making learning more flexible, creative and accessible. Explore safe ways of using technology with learners to support self-esteem, assertiveness, participation and to develop friendships. Promote and discuss 'netiquette', e-safety and digital literacy. Show learners that the adults in the school understand the technologies they use – or get the students to teach them!

5. Evaluating the impact of prevention activities

Regular reviews are vital to make sure that antibullying policies are working and are up-to-date. Consider conducting an annual survey of pupils' experiences of bullying, including cyberbullying, and a parent satisfaction survey. Publicise progress and activities to the whole-school community – keep cyberbullying a live issue and celebrate your successes!



Responding to Cyberbullying

Cyberbullying is a form of bullying, and therefore all schools should already be equipped to deal with the majority of cases through their existing anti-bullying policies and procedures. This section outlines key steps to take when responding to cyberbullying.

Supporting the person being bullied

- * Give reassurance that the person has done the right thing by telling someone, refer to any existing pastoral support/procedures and inform parents.
- * Advise on next steps:
 - Make sure the person knows not to retaliate or return the message.
 - Ask the person to think about what information they have in the public domain.
 - Help the person to keep relevant evidence for any investigation (e.g. by not deleting messages they've received, and by taking screen capture shots and noting web addresses of online cyberbullying instances).
 - Check the person understands simple ways to prevent it from happening again, e.g. by changing contact details, blocking contacts or leaving a chatroom.
- * Take action to contain the incident when content has been circulated:
 - If you know who the person responsible is, ask them to remove the content;
 - Contact the host (e.g. the social networking site) to make a report to get the content taken down.
 - Use disciplinary powers to confiscate phones that are being used to cyberbully. Ask the pupil to tell you who they have sent messages on to.
 - In cases of illegal content, contact the police, who can determine what needs to be kept for evidential purposes.

Investigating incidents

All bullying incidents should be properly recorded and investigated. Cyberbullying can be a very serious matter and can constitute a criminal offence. In UK law, there are criminal laws that can apply in terms of harassment or threatening and menacing communications.

- * Advise pupils and staff to try and keep a record of the bullying as evidence. It can be useful to show parents, teachers, pastoral care staff and the police, if necessary, what has happened.
- * Take steps to identify the bully, including looking at the school systems, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary. The police will need to be involved to enable the service provider to look into the data of another user.

Working with the bully and sanctions

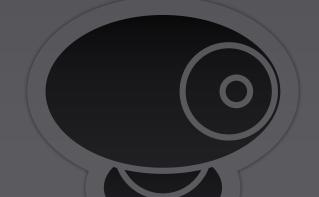
Once the person bullying is identified, steps should be taken to change their attitude and behaviour as well as ensuring access to any support that is required. Factors to consider when determining the appropriate sanctions include:

- * The impact on the victim: was the bully acting anonymously, was the material widely circulated and humiliating, how difficult was controlling the spread of the material?
- The motivation of the bully: was the incident unintentional or retaliation to bullying behaviour from others?

Technology-specific sanctions for pupils engaged in cyberbullying behaviour could include limiting internet access for a period of time or removing the right to bring a mobile into school.

'Thankfully, my son's school was very helpful: they identified the child who posted the video from another video he had posted; they have disciplined the other child and had him remove the video'.

A parent



Key Safety Advice

The whole school community has a part to play in ensuring cyber safety. Understanding children and young people's online lives and activities can help adults respond to situations appropriately and effectively. Asking children and young people to show adults how technologies and services work is a useful strategy that can provide an important learning opportunity and context for discussing online safety.

For children and young people

- 1: Always respect others be careful what you say online and what images you send.
- 2: Think before you send whatever you send can be made public very quickly and could stay online forever.
- 3: Treat your password like your toothbrush keep it to yourself. Only give your mobile number or personal website address to trusted friends.
- **4:** Block the bully learn how to block or report someone who is behaving badly.
- 5: Don't retaliate or reply!
- **6:** Save the evidence learn how to keep records of offending messages, pictures or online conversations.
- 7: Make sure you tell:
 - an adult you trust, or call a helpline like ChildLine on 0800 1111 in confidence;
 - the provider of the service; check the service provider's website to see where to report incidents;
 - your school your teacher or the anti-bullying coordinator can help you.

Finally, don't just stand there – if you see cyberbullying going on, support the victim and report the bullying. How would you feel if no one stood up for you?





For parents and carers

- 1: Be aware, your child may as likely cyberbully as be a target of cyberbullying. Be alert to your child seeming upset after using the internet or their mobile phone. This might involve subtle comments or changes in relationships with friends. They might be unwilling to talk or be secretive about their online activities and mobile phone use.
- 2: Talk with your children and understand the ways in which they are using the internet and their mobile phone. See the seven key messages for children (on the left) to get you started.
- Use the tools on the service and turn on in-built internet safety features.
- 4: Remind your child not to retaliate.
- **5:** Keep the evidence of offending emails, text messages or online conversations.
- 6: Report cyberbullying:
 - Contact your child's school if it involves another pupil, so that they can take appropriate action.
 - Contact the service provider.
 - If the cyberbullying is serious and a potential criminal offence has been committed, you should consider contacting the police.



How is Technology Used to Bully?
Technology can be used both positively and negatively. The table below explores the range of ways today's technology can be used.

Technology:	Great for:	Examples of misuse:
Mobile phones	Keeping in touch by voice or text, taking and sending pictures and film, listening to music, playing games, going online and sending emails. Useful in emergency situations and for allowing children a greater sense of independence.	Sending nasty calls or text messages, including threats, intimidation, harassment. Taking and sharing humiliating images. Videoing other people being harassed and sending these to other phones or internet sites.
Instant Messenger (IM)	Text or voice chatting live with friends online. A quick and effective way of keeping in touch even while working on other things.	Sending nasty messages or content. Using someone else's account to forward rude or mean messages via their contacts list.
Chatrooms and message boards	Groups of people around the world can text or voice chat live about common interests. For young people, this can be an easy way to meet new people and explore issues which they are too shy to talk about in person.	Sending nasty or threatening anonymous messages. Groups of people deciding to pick on or ignore individuals. Making friends under false pretences – people pretending to be someone they're not in order to get personal information that they can misuse in a range of ways – e.g. by spreading secrets or blackmailing.
Email	Sending electronic letters, pictures and other files quickly and cheaply anywhere in the world.	Sending nasty or threatening messages. Forwarding unsuitable content including images and video clips, or sending computer viruses. Accessing someone else's account, e.g. to forward personal emails or delete emails.
Webcams	Taking pictures or recording messages. Being able to see and talk to someone live on your computer screen. Bringing far-off places to life or video conferencing.	Making and sending inappropriate content. Persuading or threatening young people to act in inappropriate ways. Using inappropriate recordings to manipulate young people.
Social network sites	Socialising with your friends and making new ones within online communities. Allowing young people to be creative online, even publishing online music. Personalising homepages and profiles, creating and uploading content.	Posting nasty comments, humiliating images / video. Accessing another person's account details and sending unpleasant messages, deleting information or making private information public. Groups of people picking on individuals by excluding them. Creating fake profiles to pretend to be someone else, e.g. to bully, harass or get the person into trouble.
Video hosting sites	Accessing useful educational, entertaining and original creative video content and uploading your own.	Posting embarrassing, humiliating film of someone.
Virtual Learning Environments (VLEs)	School site, usually available from home and school, set up for tracking and recording student assignments, tests and activities, with message boards, chat and IM.	Posting inappropriate messages or images. Hacking into someone else's account to post inappropriate comments or delete schoolwork.
Gaming sites, consoles and virtual worlds	Live text or voice chat during online gaming between players across the world, or on handheld consoles with people in the same local area.	Name-calling, making abusive / derogatory remarks. Players may pick on weaker or less experienced users, repeatedly killing their characters.
(+ i!)	Virtual worlds let users design their own avatars – a figure that represents them in the virtual world.	Forwarding unwanted messages to other devices in the immediate vicinity.

When and How to Contact the Service Provider:



All UK mobile phone operators have nuisance call centres set up and / or procedures in place to deal with such instances. They may be able to change the number of the person being bullied. Mobile operators cannot bar a particular number from contacting a phone, but some phone handsets do have this capacity. Action can be taken against the bully's phone account (e.g. blocking their account) only with police involvement.

Contacts:

O2: ncb@o2.com or 08705214000.

Vodafone: 191 from a Vodafone phone or 08700700191 for Pay Monthly customers and 08700776655 for Pay as you Go.

3: Call 333 from a 3 phone or 08707330333.

Orange: Call 450 on an Orange phone or 07973100450 for Pay as you Go, or 150 or 07973100150 for Pay Monthly. **T-Mobile:** Call 150 on a T-Mobile phone or 08454125000.

Social networking sites (e.g., MySpace, Bebo, Facebook):

It is good practice for social network providers to make reporting incidents of cyberbullying easy, and thus have clear, accessible and prominent reporting features. Many of these reporting features will be within the profiles themselves, so they are 'handy' for the user. If social networking sites do receive reports about cyberbullying, they will investigate and can remove content that is illegal or breaks their terms and conditions in other ways. They can delete the accounts of those who have broken the rules.

Contacts of some social network providers:

Bebo: Reports can be made by clicking on a 'Report Abuse' link located below the user's profile photo (top left-hand corner of screen) on every Bebo profile page. Bebo users can also report specific media content (i.e. photos, videos, widgets) to the Bebo customer services team by clicking on a 'Report Abuse' link located below the content they wish to report.

MySpace: Reports can be made by clicking on the 'Contact MySpace' link at the bottom of every MySpace page and selecting the 'Report Abuse' option. Alternatively, click on the 'Report Abuse' link located at the bottom of each user profile page and other user generated pages. Inappropriate images can be reported by clicking on the image and selecting the 'Report this Image' option.

Facebook: Reports can be made by clicking on the 'Report' link located on pages throughout the site, or by email to abuse@facebook.com.

Video-hosting sites:

It is possible to get content taken down from video-hosting sites, though the content will need to be illegal or have broken the terms of service of the site in other ways. On YouTube, perhaps the most well-known of such sites, it is possible to report content to the site provider as inappropriate. In order to do this, you will need to create an account (this is free) and log in, and then you will have the option to 'flag content as inappropriate'. The option to flag the content is under the video content itself. YouTube provides information on what is considered inappropriate in its terms of service.

See www.youtube.com/t/terms.

Instant Messenger

(e.g., Windows Live Messenger or MSN Messenger):

It is good practice for Instant Messenger (IM) providers to have visible and easy-to-access reporting features on their service. Instant Messenger providers can investigate and shut down any accounts that have been misused and clearly break their terms of service. The best evidence for the service provider is archived or recorded conversations, and most IM providers allow the user to record all messages.

Contacts of some IM providers:

MSN: When in Windows Live Messenger, clicking the 'Help' tab will bring up a range of options, including 'Report Abuse'.

Yahoo!: When in Yahoo! Messenger, clicking the 'Help' tab will bring up a range of options, including 'Report Abuse'.

Chatrooms, individual website owners / forums, message board hosts:

It is good practice for chat providers to have a clear and prominent reporting mechanism to enable the user to contact the service provider. Users that abuse the service can have their account deleted. Some services may be moderated, and the moderators will warn users posting abusive comments or take down content that breaks their terms of use.

Conclusion

Technology is great and offers fantastic opportunities for children. However, the technology can be misused, and this can be very painful for those, both children and teachers, who are the targets of cyberbullying. Adults need to help children and young people prepare for the hazards whilst promoting the many learning and social opportunities available.

Tackling cyberbullying will be an ongoing process as technology continues to develop. If you would like the full guidance produced by the DCSF and Childnet, see:

www.teachernet.gov.uk/publications www.digizen.org

'Bullying in any form is unacceptable and with new technology comes new forms of bullying such as cyberbullying. Action is needed to address cyberbullying and this guidance together with its accompanying resources will play a key role in helping the school community identify what cyberbullying is, what impact it can have on its victim and outline ways in which to tackle it.'

Baroness Delyth Morgan
Parliamentary Under Secretary of State
for Children, Young People and Families

'The benefits of the internet and new technologies for children are enormous, however, bullying via technology can cause real pain. We hope this guidance and accompanying resources which Childnet has produced will be of practical use and help us all prevent and respond to cyberbullying'.

Will Gardner
CEO, Childnet International



You can download this publication or order copies online at www.teachernet.gov.uk/publications. Search using the ref: DCSF-00685-2007. Copies of this publication can also be obtained from: DCSF Publications, PO Box 5050, Sherwood Park, Annesley, Nottingham NG15 0DJ. Tel: 0845 60 222 60; fax: 0845 60 333 60; textphone: 0845 60 555 60. Please quote ref: 00685-2007LEF-EN; ISBN: 978-1-84775-043-3.

Crown Copyright 2007

This document has been written by Childnet International (a registered charity in the UK no. 1080173) for the DCSF. Extracts from this document may be reproduced for non-commercial research, education or training purposes on the condition that the source is acknowledged. For any other use please contact https://example.com/



Trust me



Thinking critically about what you see online

Trust Me is a new resource designed to support primary and secondary school teachers in exploring critical thinking online.

Developed in partnership with the London Grid for Learning to address the emerging area of online extremism and propaganda, this practical resource aims to provoke discussion among pupils so as to challenge them to think critically about what they see on websites and social media as well as the communication they have with others online.

The resource is formed of two sets of lesson plans; one set aimed at educating upper KS2 pupils at primary, the other set aimed at KS3 and upwards at secondary:







Two lessons covering critical thinking around content (such as websites, blogs, online adverts and search results) and contact (how others online may attempt to persuade us to follow a link, download a file or engage in other behaviour).

The lessons aim to help pupils:

- Understand that not everything online is trustworthy.
- Recognise ways that people online may seek to persuade them.
- Make decisions about what they might trust using different criteria.
- Engage in discussion about what they see and experience online.



Both packs contain practical activities and examples, along with additional guidance for teachers around the law, frequently asked questions, case studies and further sources of advice and information.

Secondary



Content



Propaganda





- Engage in discussion about what they see and



1et In partnership with



www.childnet.com/trustme onlinesafety.lgfl.net















Video Chat and Webcams





Webcams have become an increasingly popular and useful tool for young people and adults. People can now video chat face to face with family and friends through video calling services such as Skype and FaceTime, hold video conferences with more than one person on Google Hangouts and social networking sites, and even use their webcam as a barcode scanner to check the cost/trade in value of goods online. Some games consoles also allow the use of a camera to video chat or capture footage of someone playing a game.

hat do I need to know?



There are a huge number of positive uses and potential for using webcams as a tool for communication and searching for information and a number of sites and services may wish to access your webcam. The advice below can help you minimise the risks associated with webcams and video chatting.



Always consider who you are chatting to and what you are sharing with them. Sharing photos or video taken via a webcam can give away personal information. Be aware that webcam footage can also be recorded by someone and then potentially shared and uploaded anywhere online.

Online friendship

On some services you may receive chat requests from people you don't know. It's far better to stick to chatting with people you know in the offline world too; your family and friends. If a site or service has privacy settings, always make use of them to control who can contact you.

Webcam content online

Some webcam chat sites allow you to chat to and see strangers online and may put you at risk of seeing pornographic content or adult behaviour on webcam. This content should always be reported to the website/service.

People may use webcam chat to convince you to appear naked on camera or perform sexually suggestive acts. This can then be recorded by the watcher and be potentially used to threaten or blackmail.

If someone ever asks you to do or say anything on camera that makes you feel uncomfortable then just say no and tell an adult you trust.

Remember it is never too late to tell someone.

You can also block or report a user to the website/service if they continue to harass you.

Tell someone

UK Safer Internet

If you have been the subject of inappropriate sexual contact or approach by another person via webcam or other forms of online communication then it is vital to tell a trusted adult and to report it to the police via the Child Exploitation and Online Protection Centre (www.ceop.police.uk).

Technical Advice

Emails and links

Webcams can be affected by viruses so be wary of emails and messages on social networks from strangers that invite you to click on a link or open an attachment. These may actually contain malicious files or 'trojans' which allow the stranger to control your webcam or device remotely.

Make sure that antivirus and firewall protection is kept up to date on devices that use webcams.

Think where your webcam is in the home

Make sure that webcams connected to computers are not located in bedrooms or more private areas of the house. Although it is rare, there have been cases of webcams being hacked by programs/users to take pictures or video without the owner's knowledge.

Unplugging the webcam, covering the lens or pointing it at a blank wall when not in use are good steps to take to minimise this risk, as is closing your laptop lid when not in

Know which services/sites use webcams

Sites, services and apps may ask for permission to use your webcam. Before you accept, always think carefully about why the service may want to use your camera and who may be able to see the video feed.

End calls and log out

Always make sure you end a video chat when finished and log out of the site or service. This can help prevent anyone from accessing your account or webcam without your knowledge.

Useful Links



www.childnet.com/young-people/secondary/hot-topics www.saferinternet.org.uk/advice-and-resources www.ceop.police.uk https://support.skype.com







Further advice to discuss with your child:

Privacy settings

These settings give the user the ability to control who they share particular content with, for example making a photo you post visible to Friends only or to the Public. Encourage children and young people to use the privacy tools available on the social networking site to protect their personal information and to keep their passwords private (even from their friends).

Most social networking sites give safety advice and information on their safety tools. For example see www.facebook.com/safety for more in-depth information on Facebook privacy settings.

Online Friendship

Remind them to only add people they know and trust in the offline world to their contact lists on social networking sites.



Geolocation

Young people must be aware of who they are sharing their location with. If they are accessing a social networking site via a smartphone or mobile device, they might be disclosing their location without realising it. Location services can be turned on or off within the settings of a device.



Think Before You Post

Emphasise the importance of thinking before you post something online. This can include writing a comment or sharing a picture. Discuss with them what is and isn't OK to say in a post and remind them that sometimes messages online can be misunderstood. What may start out as a harmless joke for one person, can be extremely hurtful for another individual and once something is posted online it is potentially there forever. If you are not sure, or if you wouldn't be happy for your Head Teacher to see it, it's probably best not to post it. Your online reputation can also be affected by other behaviour, such as groups you join or clicking 'likes'.





Know how to report

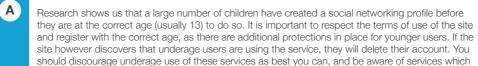
0 Know how to block other users and know how to report - make sure children and young people know how to report abusive comments or illegal activity on social networking sites. Popular social networking sites allow you to report a comment or user who is potentially breaking their terms and conditions, by clicking on a report button or sending the site an email. If young people have concerns about cyberbullying then they should speak to a trusted adult as well as saving the evidence, and even use the tools available to block other users. If you have concerns that your child is or has been the subject of inappropriate sexual contact or approach by another person, it's vital that you report it to the police via the Child Exploitation and Online Protection Centre (www.ceop.police.uk).

Logaina out

0 Once you have finished using a social networking site, it is important to log out. Specifically when using a public or shared computer and also on mobile devices. Make sure you have activated a PIN on your mobile device, as a mislaid device can mean that others can access your social networking profile.

Frequently Asked Questions

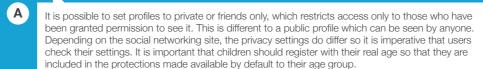
Q My child is underage, but has created a social networking profile. What should I do?



cater for younger users by having higher safety features. However, before young people start using social networking services it is important that they are equipped with the skills to stay safe online and to use social networking sites responsibly. Sit down

together and make sure that you both know how to use the privacy tools that are provided. There are multiple ways in which a social networking profile can remain private that will prevent your child from giving out personal information to strangers. Support your child in ensuring that they only add contacts to these sites that they also know and trust offline. One way to keep an eye on how your child uses a social networking site is to connect with them.

Q Can my child limit who accesses their profile?



Q Does my child's profile appear in a public search engine (eg. Google)?

This guide has been written and produced by children's charity Childnet International.

Copyright © 2013. Registered Charity no. 1080173. Copies may be ordered from www.childnet.com

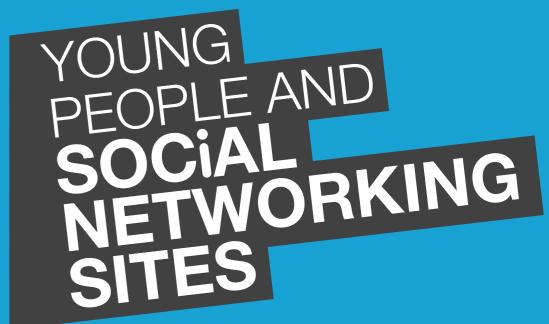


There are ways that you can prevent your profile from appearing in search engine results; most social networking sites allow you to remove your profile from public search results by using the

How can I report inappropriate behaviour and what happens when I make a report?



Social networking sites should have clear, prominent and accessible places to make a report. Providers should respond promptly to reports from users, and some will acknowledge each report with a confirmation that it has been received and provide indication of the timescale in which the complaint will be managed. Make sure you talk with your child about these tools and ensure that they know how







These types of sites allow young people to be creative online and keep in touch with their friends, as well as sharing photos and videos. On some social networks, young people can follow their favourite celebrity which means they can access the content they update and share. However, for parents and carers it's important to have a look at these services, or have a go, in order to familiarise yourself with social networking sites. Most sites stipulate a minimum user age of 13, although some interactive sites are designed specifically for younger children.



safe and constructive way, and be able to help them if they need it.





Most sites stipulate a minimum user age of 13

Social networking and your child's digital footprint

Many things can contribute to your child's digital footprint including what they post and who they interactive with. Young people are accessing and using social networking sites on a range of devices, such as mobile phones, tablets and gaming devices. They use social networking sites for many different purposes, to communicate with their friends, to share photos, to play games and to find out new information. You need to remind your child however that they need to be careful about what they're posting online and who can see it. Children can sometimes believe that social networking sites are a private space for them and it can be difficult for them to realise that actually what they're posting online may be public and can be spread very quickly and to a large audience. The blur between public and private expression can potentially put a child at risk in two main ways:

Content

Children who create or post inappropriate. offensive or even illegal content in their own or others' web pages could get them into trouble with their school, friends, or even break the law, depending on the nature of the material. It's also important that young people understand the longevity of posting something online. Once content is uploaded onto a website, it could potentially stay online forever. Regardless of whether the owner takes down the content, anyone who had access to that content could have copied it for themselves, kept it for their own records or distributed it further. Content which is uploaded online can be copied, altered and reposted by anyone and it is very difficult to 'take back' things that may be later regretted. This can damage reputations and even future prospects.



Contact

Young people need to be aware of how much personal information they upload onto these sites. If a user of a social networking site doesn't protect their information by enabling the correct privacy settings, they could be exposing their information to strangers and as a result be at risk of online contact and grooming. Posting or chatting about personal details might enable someone to identify and contact your child online or in person. There is also the more likely risk of cyberbullying with young people intentionally harming another person online. Talk to your child about protecting their privacy online and talk through the available privacy settings with them.

It's a good idea to talk to your child about their social networking life online. In the same way that you might ask them about their social life offline, talking about social networking sites together is no different. One way to get the conversation going is by asking them whether they know where to go for help, or whether they know how to make their profile private, or even ask them to help you with your privacy settings.

ڮٙڂڰ

SMART rules

As well as producing some useful conversation starters for parents and children: www.saferinternet.org.uk/ufiles/Conversation-Starters-for-Parents.pdf, Childnet has produced 5 key SMART rules which remind young people to be SMART online. It can be helpful to go through these tips with your children.



Safe

Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password.





Meeting:

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.



Accepting:

Accepting emails, Instant Messenger (IM) messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!



Reliable:

Information you find on the internet may not be true, or someone online may be lying about who they are.



T

Tell

Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.



Useful Links:

www.childnet.com/parents-and-carers/hot-topics/social-networking www.ceop.police.uk www.facebook.com/safety www.iwf.org.uk https://support.twitter.com

INFORMATION FOR SCHOOL STAFF (🐸)



1. CHILDNET RESOURCES AND WEBSITES



Childnet: Childnet International is a non-profit organisation working in partnership with others around the world to help make the internet a great and safe place for children. The Childnet website hosts all the online resources detailed below, as well as a number of recommended resources for young people, parents, carers and teachers. The Teachers and Professionals area also contains key advice, information on reporting and detailed information on a range of online safety topics in the Hot topics section. www.childnet.com



UK Safer Internet Centre: Childnet is part of the European Commission appointed UK Safer Internet Centre. Together with partners the **Internet Watch Foundation** and the **South West Grid for Learning**, we raise awareness about internet safety, develop information materials and resources and organise high profile events such as Safer Internet Day. You can access a range of resources from across the UK, Europe and wider afield at www.saferinternet.org.uk.



Cyberbullying: Understand, Prevent and Respond: Childnet's guidance is designed to support schools in understanding, preventing and responding to cyberbullying incidents involving pupils. Guidance is also included for supporting school staff with incidents.





Crossing the Line PSHE Toolkit: A practical toolkit for educators of 11-14 year olds containing films and lesson plans to explore online issues such as cyberbullying, sexting, peer pressure and self-esteem. Crossing the Line is a PSHE Association Quality Assured Resource.www.childnet.com/pshetoolkit





Trust Me: A resource created to support teachers in exploring critical thinking online. It contains lesson plans for both primary and secondary age groups based around the concept of trust and the importance of thinking critically about content on websites and social media, as well as communication online. This resource was created in partnership with London Grid for Learning. www.childnet.com/trustme





Childnet Digital Leaders Programme: The Childnet Digital Leaders Programme aims to empower pupils to champion digital citizenship and digital creativity within their schools and to educate their peers, parents and teachers about staying safe online. It offers exciting online community, structured training and ongoing support from Childnet's expert team, making online safety learning fun and effective and helping schools work towards an outstanding whole school community approach to online safety. www.childnet.com/digital-leaders



STAR Toolkit: A free resource created for KS3 & 4 educators working with young people with autism spectrum disorder. The toolkit provides practical advice and teaching activities and can be freely edited to suit the specific needs of individual young people. www.childnet.com/star



Be Safe and Smart Online: Created in partnership with The National Deaf Children's Society, these resources are designed to help and support deaf young people and their parents, carers and teachers to help them stay safe online.



www.childnet.com/resources/be-safe-and-smart-online

2. OTHER RESOURCES, ACTIVITIES & LESSON PLANS



Safer Internet Day: Free education packs are produced every year for Safer Internet Day based on the theme that year. There are packs for KS1-KS5 and Parents/Carers. Each pack includes an assembly and script, lesson plan, quick activities and promotional materials. This year's pack and previous packs can be downloaded from the UK Safer Internet Centre site.

www.saferinternetday.org.uk



ThinkUKnow: A website run by CEOP that contains information for children, parents and teachers, as well as a link for children to report abuse online. The teacher/trainer section requires sign up to access and download the resources.

www.thinkuknow.co.uk



Digital Literacy and Citizenship: The South West Grid for Learning have created free digital literacy and citizenship schemes of learning for all year groups from EYFS to KS4. These include medium term plans, individual lesson plans and links to online resources and activities.

www.digital-literacy.org.uk



Online Safety in the Computing Curriculum: This free guide produced by Childnet provides further detail to the online safety themes outlined in the computing curriculum and signposts to free high quality resources that can be used to educate pupils on a range of online safety issues.

www.childnet.com/resources/esafety-and-computing

3. INFORMATION AND ADVICE TO SHARE WITH PARENTS/CARERS





Safety Tools on Social Networks and Other Online Services:

Information and advice on the safety tools, age requirements and terms and conditions for a variety of online services popular with young people.

www.saferinternet.org.uk/safety-tools

Common Sense Media: A US non-profit organisation that provides independent reviews, age ratings and other information about movies, games, apps, TV shows, websites, books and music for families, educators and children. www.commonsensemedia.org

NetAware: NSPCC and O2 have created a guide with information and advice for parents and carers on the most popular social networks and interactive apps and games used by children and young people. The information is also available in an app for Apple and Android devices.

www.net-aware.org.uk

They also provide an online safety helpline for parents and carers to answer questions and address concerns about a child's online safety: 0808 800 5000

Net Aware))

4. PROFESSIONAL REPUTATION



Professional Reputation: The Teachers and Professionals area of the Childnet site includes a guide about your personal use of social networking sites; keeping you, the young people you work with, and your job safe.www.childnet.com/professional-reputation



Social Network Checklists: Guides produced by the UK Safer Internet Centre that contain detailed instructions and information on managing privacy and account settings on Facebook, Twitter, Snapchat and Instagram. www.saferinternet.org.uk/checklists

5. RESOURCES ON SEXTING



Sexting Resources: This page on the UK Safer Internet Centre site contains links to practical resources for educating young people about the risks posed by sexting. It also includes the guide 'So You Got Naked Online', which provides useful advice for young people on how to get help and what to do after a sexting incident. www.saferinternet.org.uk/sexting



UKCCIS: Childnet sits on the UK Council for Child Internet Safety Education Group, which has produced advice for schools and colleges on managing sexting incidents. The UKCCIS page on gov.uk also includes other outputs from the group, including guidance for school governors. https://goo.gl/3GwlxN

6. WHOLE SCHOOL DEVELOPMENT



360 Degree Safe: A free self review tool to help schools review and develop their online safety policies, procedures and provision. Sign up is required. www.360safe.org.uk



Advice Centre: The Teachers and Professionals section of the Advice Centre contains information on teaching resources, curriculum planning, policy development and a guide for schools on how to establish 'appropriate levels' of filtering and monitoring.

http://www.saferinternet.org.uk/advice-centre/teachers-and-professionals

7. WHERE TO REPORT



Need help? Information about responding to disclosures from pupils and information on where to report online concerns such as cyberbullying, inappropriate content or illegal behaviour. www.childnet.com/teachers-help



Professionals Online Safety Helpline: The UK Safer Internet Centre has been funded by the European Commission to provide a Helpline for professionals who work with children and young people in the UK, specifically tackling the area of online safety. helpline@saferinternet.org.uk 0844 381 4772



Child Exploitation and Online Protection (CEOP): A command of the National Crime Agency dedicated to tackling child abuse and child sexual exploitation. This website includes a unique facility that enables parents and young people to make reports of actual or attempted abuse online. www.ceop.police.uk



Internet Watch Foundation: Part of the UK Safer Internet Centre, the IWF is the UK's hotline for reporting illegal content found on the internet. It deals specifically with child abuse and criminally obscene images hosted in the UK and internationally.

www.iwf.org.uk

Email us:

education@childnet.com

f childnetinternational

Follow us:



Subscribe to our newsletter:

www.childnet.com

INFORMATION & ONLINE RESOURCES



1. CHILDNET RESOURCES AND WEBSITES











Childnet: Childnet International is a non-profit organisation working in partnership with others around the world to help make the internet a great and safe place for children. The Childnet website hosts all the online resources detailed below, as well as a number of recommended resources for young people, parents, carers and teachers, www.childnet.com

The Parents and Carers area also contains key advice, information on reporting and detailed information on a range of online safety topics in the Hot topics section. www.childnet.com/parents-and-carers

UK Safer Internet Centre: Childnet is part of the European Commission appointed UK Safer Internet Centre. Together with partners the Internet Watch Foundation and the South West Grid for Learning, we raise awareness about internet safety, develop information materials and resources and organise high profile events such as Safer Internet Day. You can access a range of resources from across the UK, Europe and wider afield at www.saferinternet.org.uk/parents.

KidSMART: This Childnet website is for children, teachers, parents and carers and offers fun activities for children alongside practical internet safety advice. Don't forget to check out our 'I have kids' tab where you can find links to read the online stories 'The Adventures of Smartie the Penguin' and 'Digiduck's Big Decision', which is also available as a free app for iPads and Android tablets. www.kidsmart.org.uk



INFORMATION AND TOOLS FOR PARENTS & CARERS



Supporting Young People Online: A free guide created by Childnet providing Information and advice for parents and carers on supporting young people online. The advice is also available in 12 additional languages including Arabic, Hindi, Polish, Spanish, Urdu and Welsh. www.childnet.com/resources/supporting-young-people-online



A Parents' Guide to Technology: The UK Safer Internet Centre has created this guide to answer commonly asked questions and introduce some of the most popular devices used by children, highlighting the safety tools available and empowering parents with the knowledge they need to support their children to use these technologies safely and responsibly. www.saferinternet.org.uk/parent-tech



Internet Parental Controls: The four big internet providers - BT, Sky, Talk Talk and Virgin Media provide their customers with free parental controls that can be activated at any time. Video tutorials on how to activate and use these controls are available on the UK Safer Internet Centre website. www.saferinternet.org.uk/parental-controls



Safety Tools on Social Networks and Other Online Services:

Information and advice on the safety tools, age requirements and terms and conditions for a variety of online services popular with young people. www.saferinternet.org.uk/safety-tools

3. SOCIAL NETWORKING



Young People & Social Networking Sites: Aims to help parents understand the positive and creative ways young people are using social networking spaces (e.g. Facebook, Snapchat and Instagram). It also points out the potential risks of using these sites and ways to minimise these risks. www.childnet.com/sns



Social Network Checklists: Free guides produced by the UK Safer Internet Centre that contain detailed instructions and information on privacy and account settings on Facebook, Twitter, Snapchat and Instagram. www.saferinternet.org.uk/checklists

4. MOBILE PHONES



PhoneBrain: A site created by the Phone-Paid Services Authority to educate young people and parents about phone-paid services such as calls and texts to premium rate numbers and in-app purchases. www.phonebrain.org.uk

5. FILE SHARING & DOWNLOADING



Music, Film, TV and the Internet: Childnet has developed this guide with the music, film and television industries to inform parents, teachers and young people about how to stay safe and legal when enjoying entertainment on the internet or via a mobile device. www.childnet.com/downloading

Get It Right From A Genuine Site: A UK based website created by industry representatives to help teachers, parents and other consumers know which sites are legal for streaming and downloading films, tv, ebooks, music, games and sports broadcasts. www.getitrightfromagenuinesite.org

6. ONLINE GAMING



Ask About Games: Information and advice for parents and gamers about the PEGI age rating system for video games and how to play games responsibly and safely. www.askaboutgames.com

7. OTHER USEFUL SITES FOR PARENTS & CARERS

Net Aware (1)

NetAware: NSPCC and O2 have created a guide with information and advice for parents and carers on the most popular social networks and interactive apps and games used by children and young people. The information is also available in an app for Apple and Android devices. www.net-aware.org.uk





Common Sense Media: A US non-profit organisation that provides independent reviews, age ratings and other information about movies, games, apps, TV shows, websites, books and music for families and children. www.commonsensemedia.org



Digital Parenting: The Digital Parenting website and magazines, created by Vodafone and Parent Zone, offer parents information and advice about the latest digital technologies and the challenges young people might face in their digital world. www.vodafone.com/content/parents



Internet Matters: Launched by the four major UK internet service providers (BT, Sky, TalkTalk and Virgin Media), Internet Matters is an independent, not-for-profit organisation that provides information and advice on online issues and technologies to help parents keep their children safe online. www.internetmatters.org

8. WHERE TO GET HELP & ADVICE



Need help? Information about what to do if a child comes to you for help and advice about how to report online concerns such as cyberbullying, inappropriate content or illegal behaviour. www.childnet.com/parents-help



Tackling difficult conversations: The Parents and Carers section of the Childnet website includes advice and resources on how to talk to children and young people about online safety issues. This section also includes a template family agreement and conversation starters that can be used to help families discuss how to stay safe online.www.childnet.com/have-a-conversation



NSPCC: The NSPCC has partnered with O2 to provide an online safety helpline for parents and carers to answer questions and address concerns about a child's online safety: 0808 800 5000



Children can talk to someone for advice and support at any time by contacting Childline on 0800 1111 or chatting to a counsellor online at www.childline.org.uk



Family Lives: A national family support charity providing help and support in all aspects of family life. Useful advice and information is available online at www.familylives.org.uk and they provide a free confidential helpline on 0808 800 2222.



Young Minds: The UK's leading charity committed to improving the wellbeing and mental health of children and young people. Information and advice for young people and parents/carers can be found at youngminds.org.uk and they also offer a free confidential helpline for parents on 0808 802 5544.

9. WHERE TO REPORT



Child Exploitation and Online Protection (CEOP): A police agency tackling child abuse on the internet. This website includes a unique facility that enables parents and young people to make reports of actual or attempted abuse online. www.ceop.police.uk

CEOP's Think U Know website contains information for children and parents, as well as a link for children to report abuse online. www.thinkuknow.co.uk



Internet Watch Foundation: Part of the UK Safer Internet Centre, the IWF is the UK's hotline for reporting illegal content found on the internet. It deals specifically with child abuse and criminally obscene images hosted in the UK and internationally, www.iwf.org.uk

ParentPort: A website run by the UK's media regulators, allowing you to report content unsuitable for children found in a programme, advert, film, video game, newspaper/magazine or other forms of media. www.parentport.org.uk

Email us:

Follow us:

Subscribe to our newsletter:













Useful Online Resources

1. We recommend visiting the following sites:

Safe Network

Safe Network provides safeguarding information related to activities outside the home – from after school art clubs to weekend reading groups:

http://www.safenetwork.org.uk/news_and_events/news_articles/Pages/whats-the-problemguide-parents.aspx

NSPCC

http://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/

A short video from the NSPCC on how to stay safe online: I Saw Your Willy - Be Share Aware - NSPCC

www.youtube.com/watch?v=sch WMjd6go

ChildLine

A private and confidential service for children and young people up to the age of 19. http://www.childline.org.uk/explore/onlinesafety/pages/sexting.aspx

Child Exploitation & Online Protection (Thinkuknow)

http://www.thinkuknow.co.uk

Association of Child Police Officers guidelines on sexting;

http://ceop.police.uk/Documents/ceopdocs/externaldocs/ACPO Lead position on Self-Taken Images.pdf

CEOP (Child Exploitation and Online Protection Centre)

CEOP work with child protection partners across the UK and overseas to protect children from harm online and offline:

www.ceop.police.uk

Video which shows the consequences of sharing images:

https://www.thinkuknow.co.uk/parents/Secondary/Conversation-Starters/Go-to-themovies/Exposed/

2. Internet Parental Controls

Below are links to internet parental controls for some of the biggest internet providers:

RT

http://home.bt.com/tech-gadgets/internet/stay-safe-with-bt-parental-controls-11363887238413

Sky

http://www.sky.com/shop/broadband-talk/broadband-shield/staying-safe-online

Talk Talk

http://www.talktalk.co.uk/security/homesafe-demo.html

Virgin Media

http://store.virginmedia.com/discover/broadband/your-broadband/protect-family/parental-controls.html