Parent Internet Safety Leaflet

READY TO LEARN EVERY DAY!

Hints and Tips for Parents:

- Technology is constantly changing and young people are continually learning - keep up to date on latest developments so you know about the risks
- Online safety applies to all types of devices - PCs, laptops, tablets, smartphones, e-readers and online gaming
- As technology becomes more portable, set guidelines for where your child could/should use their device
- Treat online safety in the same way as you would offline safety such as stranger danger, crossing the road etc
- Set up internet security so children can't access websites with adult and inappropriate content
- Don't write anything online that you wouldn't say in person. Comments made on social media and/or public web pages/forums could reflect badly on your child
- Check out the IT policies, particularly the online safety policy, issued by your child's school and adhere to them
- Cyber bullying should be treated in the same way as other forms of bullying; contact your child's school to agree a plan for dealing with it
- Try to establish a system which allows your child to talk to you about anything they feel uncomfortable about online

This joint NAHT and Family Action leaflet has been complied using the expertise of both NAHT members and Family Action staff. The internet can play an important part in many aspects of school life, including teach, learning and improving communication. However, if not used properly, it can be dangerous or harmful.

This simple guide includes hints and tips for both parents and pupils.

Things to Discuss with Children:

- Where is it acceptable to use your portable device? Bedroom? School?
- Who should you talk to if you feel uncomfortable about something you have seen online? e.g. parent, teacher or other responsible adult
- Don't spend too long online; make sure you get some physical exercise every day
- Keep passwords safe – don't write them down and change them regularly
- What personal information is it appropriate to post online?
- How do you report cyber bullying? Take a screen grab of any posts so these can be seen at a later date if needed
- How do you know the people you are talking to online, are who you think they are?
- What is the difference between a 'real life' friend and an 'online friend'
- When is it sensible to meet up with an online friend?

THE DIGITAL UNIVERSE OF YOUR CHILDREN

ONLINE TIPS FOR PARENTS

PRIVACY ON SOCIAL NETWORKS

Social networking sites (SNS) allow people around the world to share information. But how can you help your children stay safe when they socialise online? It may seem difficult to protect their personal details on SNS, but a few simple clicks will make sure that some important privacy settings are in place.

1 PUBLIC OR PRIVATE

By default, on most SNS your child's profile will only have a minimum level of privacy protection. There are two basic settings:

- **Public:** "Everything can be seen by everybody"
- **Closed or Private:** "Nobody can see anything, unless you want them to"

The first step towards protecting your children's privacy is to encourage them to choose a "closed" or "private" profile. Simple!

2 BLOCKING

Secondly, your children need to decide who they will allow to see their profile. Encourage them only to accept people they know to become their friends. If they do come across an unwanted contact, they can always block this person from their account.

3 TESTING THE SETTINGS

In the real world the amount of personal information we want to share with someone depends on who we're actually talking to. The same approach should apply to your child's social media profile. Most SNS give people the opportunity to decide how much information they want to share with certain groups, circles or communities. Many SNS have the option to check 'privacy settings' by allowing users to view their own profile as someone else. In this way, they can clearly see if any unwanted information appears on their profile.

4 TAKING CONTROL OF TAGGING

Protecting privacy isn't just about protecting the information your children put on a SNS. Other people can also publish images and videos and link their name to this content without their permission. This is better known as 'tagging'. Most SNS allow users to disable the tagging feature or have the option to ask the users' approval for each piece of content tagged. Encourage your children to add this setting so they can be in control of their online reputation.

5 SCREENING SENSITIVE INFORMATION

Last but not least: If it's really sensitive information, tell your children not to post it online! **Download the 'personal information' tip sheet for more information.**

NEED MORE INFORMATION?

Facebook's privacy policy:
www.facebook.com/about/privacy/

Facebook's helpcenter on privacy:
www.facebook.com/help/privacy

Find out more from the Insafe network:
www.saferinternet.org

insafe European Schoolnet LIBERTY GLOBAL

THE DIGITAL UNIVERSE OF YOUR CHILDREN

ONLINE TIPS FOR PARENTS

ONLINE GAMING

Online gaming can have a positive influence on the development of your children. However, it's essential to find a good balance between gaming and other daily activities. It's also recommended to keep an eye on the content of the games played by children, to make sure they're safe. To ensure games are right for your children – why not try them out for yourself!

FACTS ABOUT ONLINE GAMING

1. 83% of all children worldwide play games online.
2. According to the EU Kids online survey, playing games is the **second favorite online activity**. Suprisingly 'Doing homework' comes first!
3. Games require children to stick to rules and follow directions, they can actually **increase their capacity for self-discipline and autonomy**.
4. One in four 11 to 16 year old children say that **mature-rated games are their favorite**.
5. There is **no evidence** to prove that playing violent video games causes any **lasting increase in aggressiveness or violence.**

AGE APPROPRIATE GAMES

Even non-experienced gamers can select the right games thanks to the Pan-European Game Information (PEGI) age rating system, which is now used throughout most of Europe.

The PEGI label appears on the front and back of offline computer games, providing a description of the content and one of the following age levels: 3, 7, 12, 16 and 18.
The descriptive labels explain why a game has received a particular age rating. There are eight such descriptors: violence, bad language, fear, drugs, sex, discrimination, gambling and online gameplay with other people. The age levels give parents an understanding of the suitability of the game content for children, but do not take into account the difficulty level or skills needed to play a game.

With the rise in **online gaming**, PEGI recently created an online logo, which any gameplay service provider can display providing that the website meets the requirements set out in the PEGI Online Safety Code (POSC). These requirements include the obligation to keep the website free from illegal and offensive content or any undesirable links created by users, as well as measures protecting young people while they play games.

TIPS FOR ONLINE GAMING

- Limit the time your children spend playing games.
- Find a healthy balance between gaming and other activities such as meeting friends.
- Decide if the content of a game is fit for your child by looking at the PEGI symbols.
- Set strict rules about making purchases while playing online.
- When playing online multiplayer games, make sure your children do not share personal information.
- Try out the games yourself and possibly play together with your child. You may find you actually enjoy it!

NEED MORE INFORMATION?

PEGI:
www.pegi.info/en/

The 'Good Gaming Guide':
www.pegi.info/en/index /id/media/pdf/241.pdf

Videogamers in Europe 2010: Interactive Software Federation Europe:
www.isfe.eu/sites/isfe.eu/files/video_gamers_in_europe_2010.pdf

Find out more from the Insafe network:
www.saferinternet.org

insafe European Schoolnet LIBERTY GLOBAL

THE DIGITAL UNIVERSE OF YOUR CHILDREN

ONLINE TIPS FOR PARENTS

BLOCKING

Whilst your children are online they may come across websites displaying inappropriate pop-ups and advertisements. It's important to teach your child how to delete pop-ups. Knowing how to block a website can stop them from being targeted by spammers who use adware and popups to attack their computer. Try visiting some of your children's favourite websites to find out if personal data is shared and if there are any inappropriate advertisements. There are two options which can help you to control the content your children see when they are online:

1 FILTERING AND BLOCKING

You can choose to **filter and block** any content you may find inappropriate for your child. You can prevent access to certain websites, words and images in order to avoid children coming across inappropriate content. Depending on the level of security requested, you can either adjust your web browser or use internet filtering software.

Adjusting the settings of your internet browser is the easiest way to block certain websites. When working with Internet Explorer, '**open browser**' and select '**tools**' on top of the page. Select '**internet options**' and look for the '**privacy**' tab. Under the privacy window, a button called '**sites**' can be selected, where the address of the unwanted site can be entered. This process will be different for other browsers, but can be easily found online. Please note that changing browser settings is not always 100% effective, so you may want to consider buying additional filtering and blocking software, which offers more extensive options of parental control. To help you make a well-informed decision on which tool would best fit your needs, you can see the **SIP Bench II website** of the European Commission. There you'll find the results of a helpful study on parental control tools.

2 MONITORING

You may prefer not to limit the online activity of your children but instead to monitor what they do on the internet. This way children are free to discover the online world on their own, while being supervised so you can step in when necessary. Depending on the level of monitoring, you may be able to track the names and nature of all websites visited, view any posts made on social networking sites, read online chats and instant messaging conversations and even scan your children's emails.

While parent's cannot always maintain a daily review of their child's online activity, most monitoring software offers the possibility to receive a warning signal when a certain website was visited, or specific content was published. Monitoring tools are not usually provided by a browser so they would need to be purchased.

Regardless of the choice you make to either monitor and/or use filtering software, you also need to decide whether you do so with or without your child's knowledge. It is important to weigh up the benefits and disadvantages of a certain level of control and to take into account the personality and age of your child. Very young children are most vulnerable as they usually lack the social skills to detect certain dangers when online, and are more easily startled when they come across harmful information. When dealing with the youngest, it is sensible to take measures to block unwanted content.

Though parental control might work well for young children, the situation is different for teenagers. With more online experience, they can more easily get around any controls that you may set in place. Moreover, teenagers are constantly striving for independence and the freedom to develop at their own pace. Secret monitoring or blocking of information without their consent might end up having the reverse effect. Teach teenagers how they can responsibly 'personalize their internet experience' by blocking unwanted websites and content. Give them the necessary skills to be good digital citizens and surf the web in a safe, comfortable manner.

NEED MORE INFORMATION?

SIP Bench II website:
www.sipbench.eu

Find out more from the Insafe network:
www.saferinternet.org

ins@fe European Schoolnet LIBERTY GLOBAL

THE DIGITAL UNIVERSE OF YOUR CHILDREN

ONLINE TIPS FOR PARENTS

RISKS ONLINE

The best defences against online risks are openness, awareness and education. Talk with your children about their online lives, share their experiences and learn from them. Help them to use technology positively and responsibly, and give them boundaries, guidance and support. Below are a number of risks that you can talk to your children about:

1 IDENTITY THEFT

Identity theft is the theft of personal data to impersonate an individual, usually for financial gain. The issue isn't new, but has been intensified by the internet, giving criminals new routes to gather personal data on a much larger scale. Criminals use a variety of methods to gather personal data ranging from harvesting data already published online (such as on online profiles and social networking sites) to using a combination of spam, phishing and pharming techniques. The best prevention against identity theft is, without a doubt, to advise your child not to publish personal details such as bank account number(s), addresses, telephone numbers, passport details etc.

2 SPAM, PHISHING AND PHARMING

Spam emails are unwanted messages that are typically distributed in bulk. Spam messages may contain commercial content such as pornography, pharmaceuticals, dubious financial transactions, or 'too good to be true' offers.

Phishing attacks are where users are sent emails tricking them into 'updating' their personal details online via a fake website (i.e. imitating a bank). These websites save this personal information and use it for other damaging objectives.

Pharming is the process of redirecting users to a fraudulent copy of a legitimate website, again with the aim of stealing personal data and passwords for criminal intent. Talk to your children about how to identify phishing and pharming attacks.

3 GROOMING

Child grooming refers to all activities deliberately undertaken to befriend and establish an emotional connection with a minor. The aim of this 'special relationship' is to lower the child's inhibitions in preparation of sexual abuse or exploitation. Child grooming may be used to lure minors into illicit businesses such as child prostitution or child pornography.

4 CYBERBULLYING

Cyberbullying is the use of technology to deliberately hurt, upset, harass or embarrass someone else. Cyberbullying can occur using practically any form of connected media, from nasty text and image messages using mobile phones, to unkind blog and social networking posts, or emails and instant messages, to malicious websites created solely for the purpose of intimidating an individual.

Cyberbullying can be even more harmful than normal forms of bullying in several ways. As there is a:

- Possibility to electronically invade the home and personal space of the victim.
- Greater potential size of the audience.
- Greater speed of spreading upsetting messages or images.
- Difficulty in controlling anything posted or circulated electronically.
- Perceived anonymity to Cyberbullying, due to its faceless nature which can lead to children becoming involved in activities that they wouldn't dream of in the real world, whether as the perpetrator or as a bystander.

Let your children know that it's OK to block 'buddies' or just disconnect from the website if someone or something is making them feel uncomfortable online. Ultimately, they are in control, if they do choose to block or disconnect, it's still a good idea for them to talk through the issues with a known and trusted adult: this can help children and young people to reaffirm that they acted in safe and positive way.

NEED MORE INFORMATION?

Find out more from the Insafe network:
www.saferinternet.org

insafe European Schoolnet LIBERTY GLOBAL

THE DIGITAL UNIVERSE OF YOUR CHILDREN

ONLINE TIPS FOR PARENTS

ONLINE FRIENDS

Help your children develop the knowledge and social skills to make sensible decisions about the people they meet online.

1 TOO GOOD TO BE TRUE!

Tell your children to watch out for people who are overly friendly, for example, appearing to have exactly the same taste in music, movies, actors, etc. An online predator's aim is to gain the trust of children. Predators will therefore be very kind to them at first and often pretend to be their 'soul mate'.

2 INCONSISTENCIES IN FRIENDS' STORIES

Advise your children to look out for inconsistencies in their online friends' stories. For example, they should be very cautious if one of their online friends all of a sudden turns out to be much older than they originally said. If this is the case, it's best to break all contact.

3 FOLLOW YOUR INSTINCT

Even if your child has the slightest of suspicions, they shouldn't hesitate to talk to a trusted adult.

4 CONFIDE IN A TRUSTED ADULT

Make sure your children know they can always come to you or another trusted adult if they feel threatened by someone or if they're uncomfortable because of something they encountered online. **Help them to report any concerns to the police or to the website in question.**

5 MEETING OFFLINE FRIENDS – SET THE RULES

If your children want to meet online friends in the offline world for the first time, agree on strict rules **Download the "meeting strangers" tip sheet.**

NEED MORE INFORMATION?

OnGuard Online:
www.onguardonline.gov

INHOPE:
www.inhope.org

Find out more from the Insafe network:
www.saferinternet.org

THE DIGITAL UNIVERSE OF YOUR CHILDREN

ONLINE TIPS FOR PARENTS

MEETING STRANGERS

Through the internet, children are now able to communicate with people from all over the world. Online 'friendships' can sometimes evolve into real-life friendships. This means your children may be interested in meeting virtual strangers. Depending on the age and maturity of your child, as well as the context of the meeting, you can allow your child to go to a meeting with a stranger together with a friend, instead of a trusted adult. As young people can sometimes be naive and lack the social skills to assess the intentions of the people they meet online, it's necessary for you to set clear rules about meeting strangers in real life.

SUGGESTED RULES FOR YOUR CHILDREN

1. Before meeting someone you've met online, make sure you get to know them better first. Ask them about their family, hobbies, etc. If you notice any inconsistencies in their story, or if they seem too good to be true, it's better not to meet them.

2. Tell a trusted adult (parent / family member / caretaker) that you intend to meet this person and give them details about the person's identity.

3. Tell a trusted adult (parent / family member / caretaker) where and when you are meeting and make clear arrangements on when you'll be back home.

4. It is very easy for people to pretend to be someone else online. Therefore, it's worth doing a background check by using Google search or asking your friends and family.

5. Bring a trusted adult or friend to your first meeting, they can always leave you once you have arrived at the location and feel at ease. If your online friend refuses to come to the meeting if an adult or friend is there, then this is usually a sign of trouble.

6. Arrange to meet in a public place, not at a private location. Having other people around will make it safer.

7. Make sure your phone is charged and keep it on and with you at all times.

8. Trust your intuition. If something doesn't feel right, it may be best to cut the meeting short and contact a trusted adult.

9. Meet your new friend(s) a few times under these circumstances until you are certain they really are the person you've gotten to know online.

NEED MORE INFORMATION?

Find out more from the Insafe network:
www.saferinternet.org

THE DIGITAL UNIVERSE OF YOUR CHILDREN

ONLINE TIPS FOR PARENTS

PERSONAL INFORMATION

Any information we put online will remain there forever, for anyone to see - it's almost impossible to delete! This means it's important to thoroughly consider what you and your children should reveal about yourselves on the web. You should teach your children which pieces of information should be private and also help them to understand in which situations they should share private details and when they shouldn't give anything away at all.

1 DISCLOSING IDENTITY

Your child's name, national identification number, address and phone number are very valuable for online predators and criminals. Advise your children only to give out such information as their phone number and address to trusted friends. This will, to some extent, protect them from becoming the victim of an online predator and limit the possibility of becoming a victim of cyberbullying.

2 INFORMATION DISCLOSURE ON WHEREABOUTS

Talk to your children at an appropriate age and time about avoiding giving away information about their location. This precaution goes far beyond children not revealing their address, but also involves concealing details such as where they go to school or where they play sports. It is also important to warn them not to talk about any of their travel plans, or when the home will be left unattended. Such information is the ultimate gift for thieves!

3 LOCATION BASED SERVICES

A Location Based Service (LBS) uses information on the geographical position of a mobile device to offer information and entertainment services related to the user's location. It is important to check all the active applications on your child's mobile phone and decide if they need to be disabled or not.

4 FINANCIAL INFORMATION

Inform your child that any kind of financial information such as bank account numbers should never be displayed online.

5 PASSWORDS

Warn your children that by sharing their passwords with others it can give people access to their account. Even with good friends, this is best avoided.

6 EMBARRASSING PHOTOS OR VIDEOS AND HURTFUL OR INSULTING COMMENTS

Encourage your children to think before they post things online. The online behaviour of people, including the things they post, will determine their online reputation. Remember, what they post online now will remain there forever. To avoid future disappointments (university, college and jobs), it's best to maintain a positive reputation.

NEED MORE INFORMATION?

Find out more from the Insafe network:
www.saferinternet.org

INFORMATION & ONLINE RESOURCES

1. UK SAFER INTERNET CENTRE

UK Safer Internet Centre: The European Commission appointed UK Safer Internet Centre is made up of three partners; **Childnet International**, the **South West Grid for Learning** and the **Internet Watch Foundation.** Together 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.

Registered UK Charity: 1080173

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 Parents and Carers area also contains key advice, information on reporting and detailed information on a range of e-safety topics in the **Hot topics** section.
www.childnet.com

Registered UK Charity: 1120354

South West Grid for Learning: The South West Grid for Learning (SWGfL) is a not for profit, charitable trust dedicated to the advancement of education through information and communication technologies. They provide safe, supported broadband internet, teaching and learning services for 2,500 schools in the South West of England and e-safety education and training regionally, nationally and internationally. They provide professionals, parents and children with advice, resources and support to use internet technologies safely to enhance learning and maximise potential.
www.swgfl.org.uk

Registered UK Charity: 1112398

Internet Watch Foundation: The Internet Watch Foundation 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. The IWF works in partnership with the online industry, law enforcement, government, and international partners. It is a charity and a self-regulatory body with over 100 Members from the online industry.
www.iwf.org.uk

2. SAFER INTERNET DAY

Safer Internet Day: Celebrated globally every year, Safer Internet Day offers the opportunity offers the opportunity to highlight positive uses of technology and to explore the role we all play in helping to create a better and safer online community. It calls upon young people, parents, carers, teachers, social workers, law enforcement, companies, policymakers, and wider, to join together in helping to create a better internet. Ultimately, a better internet is up to us!
www.saferinternetday.org.uk

3. FACTSHEETS/INFORMATION 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 11 additional languages including Arabic, Hindi, Polish, Spanish, Urdu and Welsh.
www.childnet.com/resources/supporting-young-people-online

Information and Advice for Foster Carers/Adoptive Parents:
The UK Safer Internet Centre has worked together with Islington Council to create leaflets for foster carers and adoptive parents. The leaflets, which are free to download and easy to print, include top tips and conversation starters to help foster carers and adoptive parents get to grips with internet safety.
www.saferinternet.org.uk/fostering-adoption

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. This advice contains top tips for parents and carers for keeping young children safe online.
www.childnet.com/resources/keeping-young-children-safe-online

4. ONLINE RESOURCES FOR PARENTS & CARERS

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 download 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

Online Gaming: Childnet's guide contains helpful advice and information on supporting children and young people playing games online.
www.childnet.com/online-gaming

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

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, Twitter and Instagram). It also points out the potential risks of using these sites and ways to minimise these risks.
www.childnet.com/sns

5. WHERE TO REPORT/GET HELP

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.saferinternet.org.uk/need-help

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

NSPCC: If you have concerns about the safety of a child then contact the NSPCC helpline on 0808 800 5000 or email help@nspcc.org.uk.
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.

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: enquiries@saferinternet.org.uk

Find us on Facebook: saferinternetuk

Follow us: @UK_SIC

Subscribe to our newsletter to stay up to date: www.saferinternet.org.uk