

E-SAFETY GUIDE

2017



Welcome to Britannica's guide to e-safety...

Here at Britannica we have long understood that while the internet opens up a whole new world of learning and discovery, it also has certain risks and dangers. That is why we are delighted to welcome you to our brand new e-Safety guide for schools, which we hope you find useful.

Research from Britannica among 11-16 year olds reveals:

- 19 per cent of students often feel unsafe when researching online.
- 40 per cent say it is “very easy” to access inappropriate material online.
- 19 per cent say their school has not taught them how to research safely online.

Whether it's updating Facebook on a smartphone, playing with online gamers at home, or researching a homework assignment on a laptop, safety concerns are always present.

We all want students to understand the risks and stay safe. This guide introduces everything that you need to know in order

to do so and brings together the very latest advice to help keep young people safe online, wherever they are and whatever device they are using.

For students this guide is intended for those in the early years of secondary school, though the information is also useful to people of all ages; including parents and teachers, and includes advice for using social networks and forums safely and avoiding risk when playing games and researching online.

We hope that you will all benefit from this guide to online safety...



Why e-safety is so important

You can do almost anything, and go almost anywhere on the internet, so stay one step ahead and be e-safe...

Just as you learn how to cross the road safely, you can also learn to use the internet safely. It's important to learn how to be safe online so that you experience the enormous benefits of the internet responsibly and with confidence.

This guide will help you to:

- Learn how to avoid upsetting or unsafe situations.
- Recognise when someone is using the internet in inappropriate or threatening ways.
- Develop confidence in dealing with uncomfortable situations.
- Discover strategies to protect the security of your computer and mobile phone.
- Stay safe when you are on social networks, playing games or researching homework.
- Know what to do if something goes wrong.

The internet offers information and entertainment for people of all age groups, faiths, cultures and nationalities. However, much of the content is aimed at and written by adults, there are many sites you may not understand, find unsuitable or inappropriate, or in the worst cases even illegal.

No matter what you use the internet for, by understanding the risks and knowing what to do if things go wrong, you can stay in control.



Useful things to remember and helpful do's and don'ts

Think before you post

Before you post a comment, image or video on the internet, think about its content. It might be funny to you and your friends, but upsetting or offensive for others.

Tell an adult and report it

You can always report something upsetting. If you see a post, website, image or video that upsets you or makes you uncomfortable, the most responsible thing you can do is to tell an adult.

Never be persuaded

Stay safe when talking to online friends. Never be persuaded to send personal things like photos or videos, or personal information.

Learn about privacy controls

No matter what you use the internet for, always investigate a website's social media channel's privacy settings, making sure you never display your date of birth, address, phone number or any other personal information.

Consider blocking

Most sites will have a block function, so you can ignore someone who is behaving inappropriately or is upsetting you.

Shut down or log off

It can be difficult to avoid seeing things you wish you hadn't. You can always shut down or log off your computer. You can then report the site to a responsible adult or to the Internet Watch Foundation at www.iwf.org.uk.

Say "no"

If you are being pressured by an online contact to do something you are not comfortable with, no matter how friendly, persuasive or even threatening they may be, always say "no" and tell an adult.

Don't be afraid

If something does go wrong, don't worry, everyone makes mistakes. If you have seen something upsetting or worried you may have made a mistake the best thing that you can do is to tell an adult and they can help to put it right.

Don't arrange to meet online "friends"

There are no exceptions to this rule. People you meet online may not be who they say they are and could even be an adult pretending to be a child. Tell an adult immediately if this happens.



Useful things to remember and helpful do's and don'ts

Don't be a victim of online bullying

Just because someone is behind a computer screen, this doesn't make jokes, teasing or taunts at someone else's expense any less upsetting. If you feel you are being bullied, report it to the site's administrator and tell an adult at once.

Do keep personal information private

Never disclose personal information when you are online. This includes your name, age, mobile number and address. You should always keep passwords private, so that only you and your parents / guardian know what they are.

Do think about what you say

The internet is a public place. You never know who might see what you are saying and doing, so think carefully about what you post. While you can hide posts, they may still be visible somewhere.

Do be careful with photos and videos

Be careful about posting photos or videos online. Once uploaded it is very difficult to control who can see a photo or video and how it will be shared. Photos and videos can sometimes "go viral" or be shared by lots of people very quickly.

Do protect your computer

Check with your parents / guardian that your computer has anti-virus software and that it's up-to-date. Don't open unknown attachments or downloads from emails or websites as they may contain viruses.

Do be careful with your mobile

Your mobile phone is just like a portable computer, so you need to apply the same "dos and don'ts". But also remember to keep your mobile number private, make sure it's got a PIN and don't reply to texts if you don't know who they are from.

Do surf the net safely

You can avoid inappropriate content or unsafe sites by ensuring "safe searches" are switched on and sticking to trusted sites. If you do see something inappropriate, let an adult know.

Do take the exit

Don't forget – you are in control of your online activity – so if at any time, you want to "exit", do so! It's only a matter of logging off and closing down.

Do learn together

You probably know more about the technology you are using than your parents. Keep them up-to-speed with how the technology works so you can enjoy the web together!



Surfing the web

With an infinite number of websites to choose from, how do you separate the good ones from the bad? By following these tips, you can navigate your way around the web as safely as possible and save a lot of time!

Tips for avoiding harmful websites

Internet filters

Ensure you have filters set up which will block sites that may be dangerous or harmful. Your parents / guardian can also contact your internet service provider (ISP) to ask about parental controls.

Never guess the address

Be specific about the website address you type when searching. This will ensure that you avoid harmful sites. If you don't know the address, then try a safe search engine.

If in doubt, don't click

If an address seems odd or is spelt wrong, don't click on the link – it's not worth the risk. See if you can find an alternative site which is trusted.

For searching the web safely

Be search savvy

Be as specific as possible when you search. Searching for “Magnetic Poles” will give better results than “Poles” for example.

Google tips

Putting search terms in quotation marks will ensure you get better results when searching for exact phrases.

Using the minus sign will eliminate certain words if you're trying to search a term that is generating lots of results.

Typing “site:” after a search term and entering a website address will search for every time that site in particular mentions your search term

Check your spelling

Spelling or typing errors can affect your searches. Check your spelling before you start to get better results.



Mobile devices

The same rules and risks apply to mobile phone and tablet use as they would on a computer. Communicating by email, voice, text or instant message is just like using the internet on your computer. But there are additional risks you should be aware of.

Protect your personal details

Never give out personal details or your location when you are on your mobile. Keep your password, phone number and any PIN safe – and never give it to anyone, apart from your parents / guardian.

Report inappropriate content

You may be sent messages, images, videos or other content that are upsetting or unsuitable. Always report any incidents to your mobile phone provider, or to a parent / guardian.

Agree on a set of rules with your parents before use

Make sure your parents / guardian let the mobile provider know you are under 18 and agree on – and stick to – how much time you will spend using the device each day.

Disable bluetooth

If Bluetooth is activated, you could receive unexpected and unwanted messages, and personal information may be visible. Don't run the risk of being "Bluejacked" (see Glossary) and turn it off.

Choose your apps carefully

Only install apps from a trusted source, such as those offered by your phone network, phone manufacturers or trusted app sites.

Do not be tempted to download apps sent to your phone by someone you don't know. Paid apps require a credit or debit card, always check with your parents / guardian before downloading or signing-up to any "in-app" purchases.

Consider insurance

Accidents happen from time to time, so talk to your parents / guardian about getting your mobile devices insured.



Social media

Swapping stories, sharing photos and keeping in touch with friends on sites across social media can be great fun! But there are certain risks and dangers that you should be aware of.

Personal information

Profile pages can display personal information. Check the account and privacy settings to see what information is being displayed about you automatically. Why not play it safe and make your profile searchable and visible only to your friends?

Keep what you post between you and your friends

Most social networking sites have security settings that prevent strangers from seeing your profile or status. Of course you want to talk to your friends, but make sure your profile is only visible to people on your friends list.

Be considerate

The golden rule is to pause before posting. If you are posting about someone else think whether it would make you upset or embarrassed if it was about you. Remember that the internet is a public space, so only post comments and pictures that you would be happy for anyone to see.

Age-restrictions

Most social networks have age restrictions. Before signing-up, check that you are old enough - don't lie to gain access.

Messages and notifications

Be very careful with emails, files or pictures sent to you by people you don't know. They could contain viruses or malware. Similarly if you receive a message from a friend which doesn't sound like them, don't click on it – they may have been hacked.

Passwords

Sometimes hackers take over social media accounts to post spam. Avoid this by giving your account a strong password and change it on a regular basis. Never show or share your password with anyone outside your family at any time.

Also make sure you have password recovery in place if your account does get hacked so you can get access back quickly.

Cyberbullying

If you are upset by something or someone on a social networking site then tell an adult. It isn't your fault and you don't have to put up with it. Cyberbullying is a crime, and something can be done about it, don't keep it to yourself.



Online gaming

Any game that you play when you are connected to the internet is an online game.

When online gaming consider the following:

- Beware of gaming sites that ask you to reveal personal details or information.
- Don't forget that you are playing with strangers, as well as with friends.
- Online gaming is often uncensored and the content may not be suitable for your age group.
- Avoid downloading cheat programmes as they can contain viruses that can damage your computer.
- Some games require a monthly fee – check with your parents / guardian before signing-up.
- Some games will ask you to pay for special privileges. Always check with your parents / guardian before giving your bank details – or theirs.
- Online gaming can be addictive – set a limit of how long you will spend playing.
- Online gaming has different risks to other forms of internet use as they often contain elements of social networking, chat rooms and forums.

Keep your real details private

Pick a username that doesn't reveal any part of your real name and never share your address, telephone numbers or age.

Create an avatar

Do not use a real photograph of yourself. Many online gaming sites allow you to create an avatar (cartoon version of yourself).

Don't arrange to meet online gamers

You never really know who you're playing with. Your gaming friends could be much older than you and very different in real life. Always tell an adult if anyone asks you to meet them.

Make your password secure

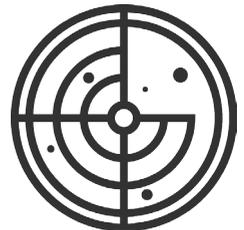
Make sure your password is "strong" and is at least eight characters long.

Beware of bullies

Online games don't always have age limits or content control and can be ideal "hiding" places for bullies. If you feel you are being bullied report them and tell an adult.

Beware of webcams and voice chat

Unless you are playing with a best friend or family member, never use a webcam for online gaming. Always remember to turn off your camera and microphone when you have finished.



Homework

Finding reliable information you can trust

You can access lots of websites with a few keystrokes – but how do you know whether the information they contain is accurate and reliable?

The internet is fantastic for helping with homework. But remember anyone can publish a page on their favourite subject. It's important to understand that not everything you read on the internet is 'true'. Some sites are not as reliable as you might think, and publish opinion rather than fact.

To make the most of the internet for your homework, remember to:

Use multiple sources

When you're researching a topic for homework, try to take your information from more than one source, just as you would use more than one book.

Check the publisher

If you're searching for information about a controversial topic – for example fox hunting – ask yourself the simple question: Who is publishing this? Groups like the Countryside Alliance and the League Against Cruel Sports will have opposite opinions and may publish "facts" that are not the same.

If you want to be sure that the information you are reading online is accurate and reliable, see if you can find out the answers to the following questions:

- Who is the author?
- Who is the publisher?
- Who is paying for the site?
- Do they know what they are talking about?
- Why are they publishing this information?
- Is their information biased in any way?
- Who links to their site?
- What date was the last update posted?



Homework

Choosing between different sources of information

If you are searching the internet for information you need for your homework then you may often switch between Google, Wikipedia and another encyclopedia like Britannica. All three can provide valuable information. But it's important to understand the differences between them and the types of information they provide.

Google

Google takes the words you enter, and finds you as many websites as possible that contain them. Some of the websites listed will be accurate and reliable, while others will not. Google is a great starting point though, and is useful for getting a range of sources together in one place.

Wikipedia

The Internet has a number of information sources referred to as 'open source' or 'crowdsourced'. This means that everything they contain has been written by people like you and me. These sites can be

valuable resources, but they aren't always the best places to find reliable information for a homework assignment. Since anyone can add or change information in these databases there is no certainty about whether they're accurate or reliable. Some information will have been entered by professional researchers. Unfortunately, some will not, and it isn't easy to decide which is which.

Britannica

Britannica is an online encyclopedia written and maintained by experienced and professional researchers. You can be sure that the information you receive is trusted, written by experts in their chosen field of expertise, fact checked and professionally edited. The content is also age appropriate for the reader.

Of course you will want to use all three websites from time to time. Each one has a useful role to play. But make sure you understand the difference between them so that you feel confident of the type of information you are searching for.



Don't be afraid...

No matter your age, the internet is virtually inescapable!

If you were to read the papers or watch the television, you could be forgiven for thinking that the internet is a dark place, full of risks and dangers. But it is used every day by millions of people of all ages for banking, shopping, travel, researching, keeping in touch and much, much more, without them coming to any harm.

Keeping you safe online is not about attempting to limit the time you spend online, or to police every page you visit or message you send.

This guide isn't intended to scare or unduly worry internet users, but to provide advice which will allow you to understand what the risks are and how best to reduce them. More important than any list or rules, however, is to encourage young people to think and to remember that being e-safe is always important.

Good luck!

We hope that you have found the information in this guide useful, and that you will use it to stay safe online.

If you've found this useful, make sure that you share the information with others; friends, parents or even teachers can benefit from the knowledge you've gained.



Useful sites

Check out the following sites we have used through this guide for more information on staying safe online:

Busy Teacher

<http://busyteacher.org/>

Child Exploitation and Online Protection

www.ceop.police.uk/safety-centre

Childline

www.childline.org.uk

The Internet Watch Foundation

www.iwf.org.uk

Virtual Global Task Force

www.virtualglobaltaskforce.com

Cyber Mentors

www.cybermentors.org.uk

Childnet

www.childnet.com

Digizen

www.digizen.org

The Department for Education

www.education.gov.uk



Glossary

Here's a list of some words and phrases which you may or may not be familiar with:

Anti-virus software - A protective program that checks the files on your computer and anything sent to you in email, chat or on a web page for viruses and other malware.

Block - Prevent a computer accessing something on the internet, or stop a program running.

Bluejacking - Sending anonymous texts to strangers using Bluetooth-enabled devices is called 'bluejacking'.

Bots - Bots can be controlled over the internet and used to send spam or steal data.

Content filter - A filter that prevents access to material on the internet by checking it is suitable before it is shown to the user.

Downloading - Copying something over the internet.

Filter - A way of preventing certain types of material from reaching your computer.

Firewall - A program that checks all the information passing between your computer and the internet to see if it is safe or permitted.

Malware - Bad software that can damage your computer (viruses) by stealing your personal information (spyware) or exposing your computer to hackers (Trojan horses).

Moderated chatroom - A chat room where an adult is watching the conversations to make sure the online behaviour is appropriate.

Parental controls - A program that parents can use to control children's access on the computer.

Password - A word or series of letters, numbers and punctuation marks that only you know, which you use to log on.

Personal Identification Number - A number, often only four digits, used like a password.

Search engine - A website that allows you to search other websites by typing in the words you are looking for.

Social networking - Social networking is a way of using the internet and the web to find, and make friends and keep in touch with people

Software - Programs that run on your computer.

Spyware - A type of malware that spies on what you are doing on your computer. It can be used to steal your passwords and login details.

Virtual - Places you visit or people you meet when you are on the internet are virtual and not "real".

Virus - A malware program that can hide itself on your computer by making changes to another program. A virus can delete your files, steal your data or even take over your computer and let hackers control it.

Webcam - A camera that is plugged into or built-in to a computer and used to send images and video over the internet.

Disclaimer

This guide is intended to be used by students within school and at home for personal use only. Britannica will permit reasonable copying, printing and sharing of this guide for personal use only. The guide remains Britannica's intellectual property.

The material and information contained in this guide are for general information purposes only. Britannica accepts no liability for the consequences of any actions taken by individuals or institutions on the basis of the information provided within this guide. You should not rely upon the material or information in this guide as a basis for making any business, legal or any other decisions. Britannica makes no representations or warranties of any kind, express or implied about the completeness, accuracy, reliability, suitability or availability with respect to the guide or the information, products, services or related graphics contained within it for any purpose. Any reliance you place on such material is therefore strictly at your own risk.

Certain links in this guide will lead to websites which are not under the control of Britannica. When you activate these you will leave this PDF. Britannica has no control over and accepts no liability in respect of materials, products or services available on any website which is not under the control of Britannica.

In no circumstances shall Britannica be liable to you or any other third parties for any loss or damage (including, without limitation, damage for loss of business or loss of profits) arising directly or indirectly from your use of or inability to use, this guide or any of the material contained in it.

These disclaimers and exclusions shall be governed by and construed in accordance with English law.

2017 Encyclopædia Britannica, Inc. Encyclopædia Britannica, Britannica and the thistle logo are registered trademarks of Encyclopædia Britannica, Inc. Third-party trade names, product names or logos referred to may be registered trademarks or trademarks of their respective owners.



britannica.co.uk

Web: britannica.co.uk | **Email:** enqbol@britannica.co.uk

Phone: +44 (0)20 7500 7800