Internet Safety Advice

Why is it important to stay safe online?

Most of us are ‘connected’ via our laptops, consoles, handheld devices, mobile phones, tablets or personal computer. The potential for the Internet to be valuable and a fun resource for entertainment, making friends, keeping in touch and learning is huge. But if you use the Internet, you could be at risk of illegal activity or abuse – be it bullying, fraud or something more serious. Unlike seeing someone face to face, on the net, people aren’t always what they first seem.

In the same way you learn about safety when you leave the house, it is important to learn how to stay safe online. These are skills that will stay with you for life.

What might I wish to prevent my family from accessing?

- Sites containing adult content, indecent images/violence and age inappropriate for the user.
- Online TV/Film sites that stream programmes and movies of all age ratings.
- Social Networking sites allowing personal information, photos messages an location to be share with other users.
- Chat site and Apps allowing private one to one or group conversations, using voice and or video
- Money lending sites offering instance cash loans without the need for credit check.
- Websites that allow the purchase of music/films/games via the users’ mobile contract.

How are these sites accessed?

- Most access to the Internet happens via a web browser such as Chrome, Firefox, Internet Explorer or Safari.
- Almost all devices now have Apps that allow the user to easily connect with other users without the need of a Web Brower such as WhatsApp, Snapchat, Facebook, Twitter, Instagram and Flickr.

Potential Risks

- When signing up for sites such as these, some personal information is required such as, name, date of birth, gender, location, telephone number, email address and sometimes a photo. Some site may also ask for a credit card to be registered, even when it’s a free service.
- Once the personal information has been obtained, it can sometimes be shared with other members of the website or App to allow contact via a chat site, email photo/video or even calls from people or organisations other than those in your group of friends or contacts.

Protecting your family when online

- Although you may have already discussed Internet safety with your family, arranged specific times for them to go online and are aware of the personal information they have uploaded, it is still extremely easy to access inappropriate and undesirable content found by search engines such as Google, Bing and Yahoo.
- These sites can return links to content that children and young people should be exposed to. The risks of this happening can be greatly minimised by change the content and privacy features and settings that most devices include.

Indecent Images – 'Sexting'

Sexting usually refers to sending and receiving rude messages or videos of:

- Naked picture
- 'underwear shots'
- Any sexual texts, images or videos

These images or videos can be sent from a boyfriend/girlfriend, a friend or someone you've met online. You also may have sent a sexual photo, video or text to someone else.

Sexting can happen because:

- Your friends are boasting about sending or having photos on their mobile phone.
- You want to fit in with friends
- You're worried about being seen as 'frigid' or 'shy'
- You're pressured to 'prove' your sexuality
- You're harassed, threatened or blackmailed into sending pictures
- Someone keeps asking for things and you feel that its easier just to 'give in'
- You're made to feel guilty if you don't do what they ask
- You think you 'owe' your boyfriend or girlfriend or;
- You feel proud of your body and want to share it with other people
- You want to have a sexual relationship with someone you have an online relationship with.

Remember:

- There is **NO** turning back once you press send.
- Even if you use apps like Snapchat the person can take a screen shot.
- You risk being seen as someone you are not.

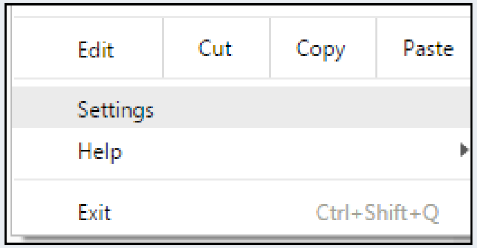
Desktops, Laptops and Tablets

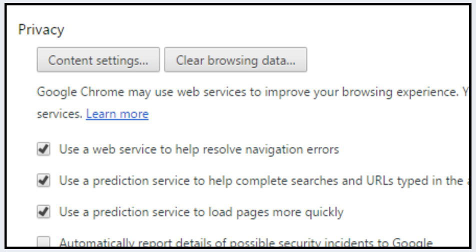
Creating a separate username for each family member will allow appropriate content settings, age rating and access to be set for each user. Users can be created or changed via the **Control Panel or Settings with the APP.**

You can install and set up parental controls offered by your Internet service provider (**ISP**) such as BT, Sky, Virgin Media etc. These will be available either online or as a software download. When set up, this allows specific content types, sites or software to be restricted unless a **Parental Password** is used.

<u>To restrict access via:</u>

- **Web Browsers – go to the Settings > Content or privacy menu of the web browser.**




Privacy

Content settings... | Clear browsing data...

Google Chrome may use web services to improve your browsing experience. Y
services. Learn more

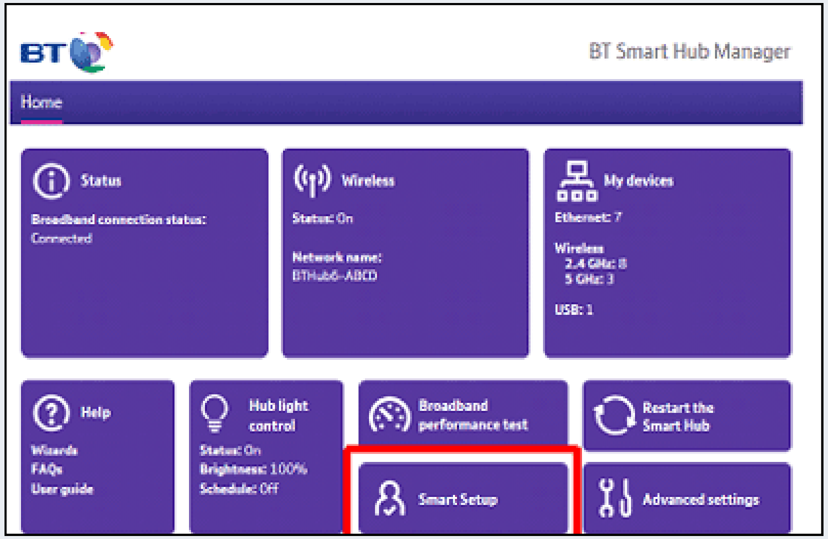
☑ Use a web service to help resolve navigation errors

☑ Use a prediction service to help complete searches and URLs typed in the

☑ Use a prediction service to load pages more quickly

□ Automatically report details of possible security incidents to Google

- **Broadband hubs and Wi-Fi routers – go to the Access Control in your Internet hub or router menu.** (Most Wi-Fi hubs or routers feature a **Wireless Off** button which can instantly disconnect all devices from the Internet but please note that devices such as mobile phones and tables with a 3G/4G connection are not reliant a Wi-Fi and will remain connected.


BT Smart Hub Manager

Home

Status
Broadband connection status:
Connected

Wireless
Status: On
Network name:
BTHub6-ABCD

My devices
Ethernet: 7
Wireless
2.4 GHz: 8
5 GHz: 3
USB: 1

Help
Wizards
FAQs
User guide

Hub light control
Status: On
Brightness: 100%
Schedule: Off

Broadband performance test

Restart the Smart Hub

Smart Setup

Advanced settings

- **Mobile Network** – contact your network provider.

Other types of Internet use

Spam, Phishing and Viruses

- Spam – unsolicited bulk messages, especially advertising.
- Phishing – the act of attempting to acquire sensitive information such as usernames, passwords and credit cards.
- Viruses/Adware/Malware – programs that may be harmful to your computer.

Emails

If you have an e-address, at some point you might receive a message from someone you don't know.

They could be:

- Selling something (this is called a 'spam' email)
- Sending you a virus
- Sending you an attachment (in most cases contact a virus, adware or malware)
- Sending abusive or explicit content.

The golden rule is, if the email is from someone you don't know, delete it.

- If it is spam, you might get ripped off.
- If it is a virus, your computer might get damaged.
- If it is an attachment, it might contain a virus, or it might be something you don't want to see. You will have to pay to remove it from your computer.
- If it is abuse or explicit, it might upset you or even get you into trouble.

You can avoid unwanted emails by installing software that prevents the above.

Useful Websites - click to open website

https://ceop.police.uk/

http://safe.met.police.uk/Internet_safety/get_the_facts.html

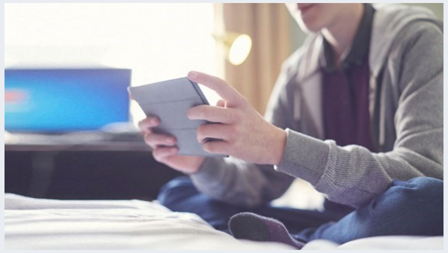
https://www.getsafeonline.org/

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

http://safe.met.police.uk/Internet_safety/other_help_and_advice.html

Some Golden Rules for Students

- Don't post any personal information online – like your address, email address or mobile number.
- Think carefully before posting pictures or videos of yourself. Once you have put a picture of yourself online most people can see it and may be able to download it.
- Keep your privacy settings as high as possible.
- Never give out your passwords.
- Do not become friends with people you do not know.
- Don't meet up with people you've met online. Speak to your parent or carer about people suggesting you do
- Remember that not everyone online is who they say they are
- Think carefully about what you say before you post something online
- Respect other people's views, even if you don't agree with someone else's views doesn't mean you need to be rude.
- If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website, turn off your computer if you want to and tell a trusted adult immediately.
- Click on the image to follow a link to childline.org.uk to get more information of how to stay safe online.



NSPCC

Safe

GET SAFE ONLINE

Get Safe Online
Free expert advice

CEOP
A National Crime Agency command