Online safety

What is it?
What are the risks?
How do I keep my child(ren) safe?
How do I report concerns?
Where can I get information?

Online safety

- Utilising information and communication technologies in a safe and responsible way.

or

- Awareness and ability to remain safe and act responsibly when using e-mail, internet, apps, smart phones, games consoles and any online method of communication.

Some methods of communication

- Facebook
- Twitter
- Tumblr
- Snapchat
- Instagram
- WhatsApp
- Youtube
- Anonymous chat apps
- Games consoles and online gaming sites e.g. steam

Potential risks

- Bullying by peers and people you consider "friends".
- Posting personal information that could identify you.
- Sexual grooming, luring , exploitation and abuse by strangers.
- Exposure to inappropriate content.
- Exposure to racist or hate material.
- Encouragement of violent behaviour, such as 'happy slapping'.
- Glorifying activities such as drug taking or excessive drinking.
- Risk of physical harm in making video content.
- Running away from home as a result of contacts made online.
- Radicalisation and exposure to extremist views.

Devices

Through secondary school mobile phones and laptops become the most popular devices for accessing the internet.
69% of 11-12 year olds use a mobile phone, compared to 83% of 15-17 year olds.
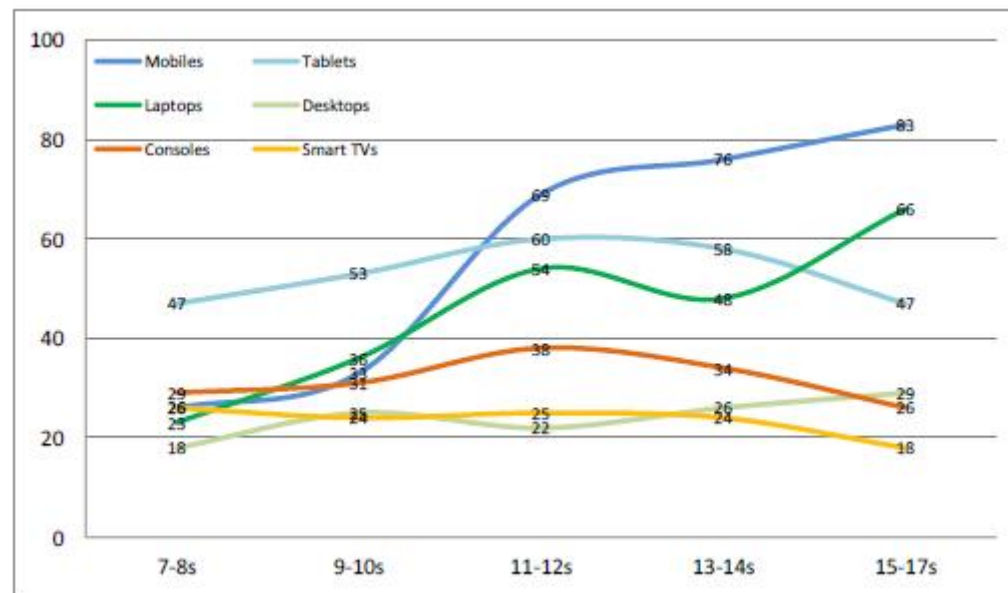
Source; pace of change report 2015

Time spent online

- Children between the age of 7 and 17 claim to spend twice as long online as their parents.
- Children using mobile phones and games console spend, on average, approximately 3 hours per day online.
- Girls device of choice is a mobile phone.
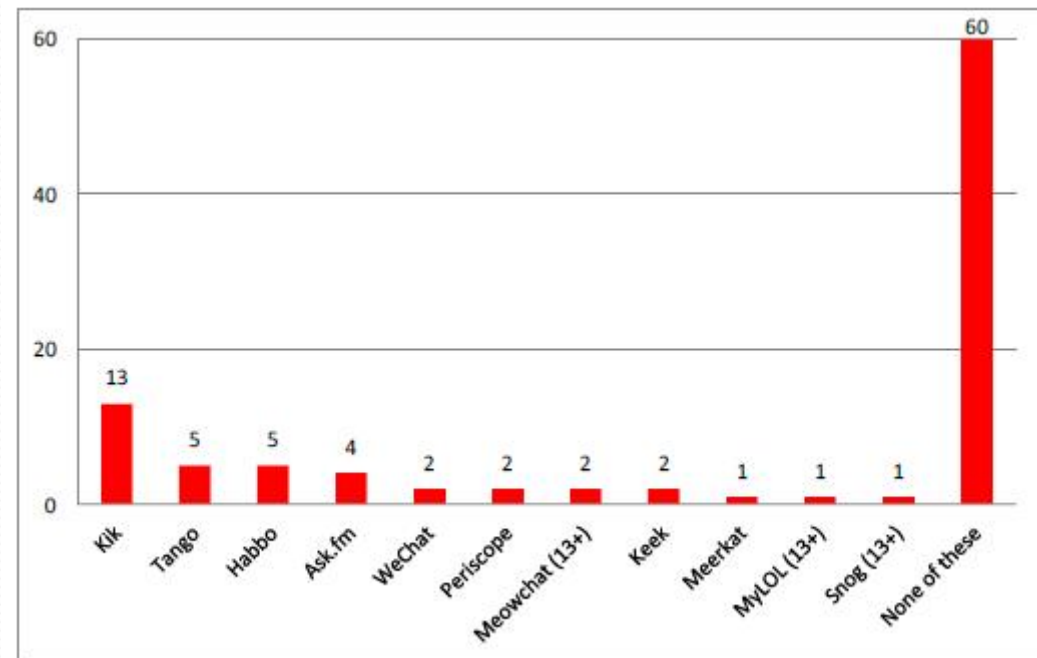- Boys spend longer than girls on other devices.
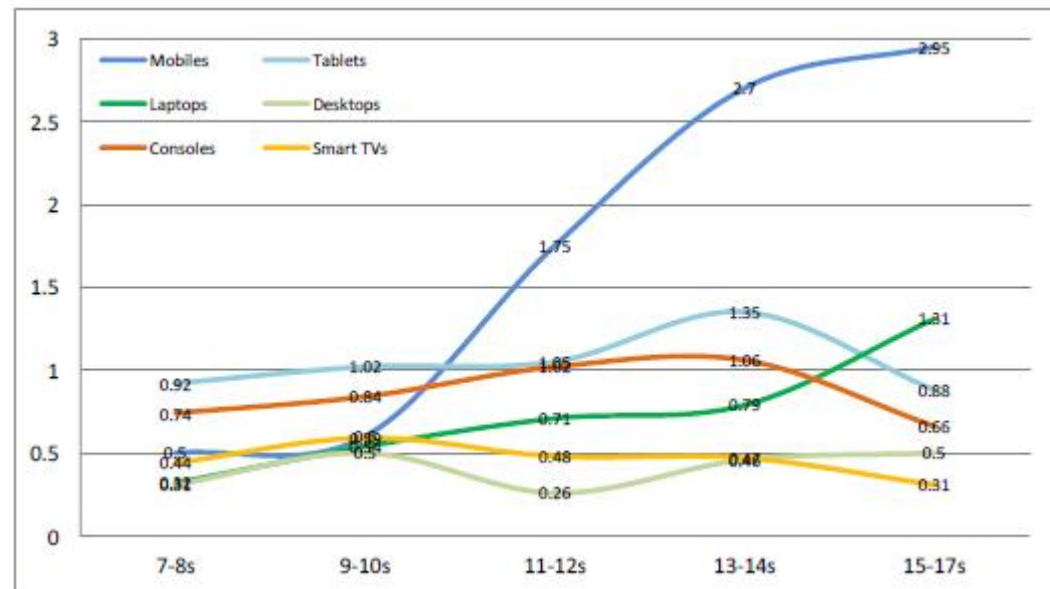
Source; pace of change report 2015

Reasons for going online

- The most popular reasons for children to go online on a normal day are;

1. Using a social networking site (2.8 hours)
2. Listening to music (2.4 hours)
3. Playing games (2.3 hours)
4. Messaging friends / family (2.3 hours)
5. Watching video clips (2.1 hours)

- 62% of 11 year olds and 69% of 12 year olds have a facebook profile
- 4 out of 10 children remove privacy settings to attract more friends or followers.
- On average children attract 100 followers to every one of their profiles – yet six out of 10 of them are not real friends.
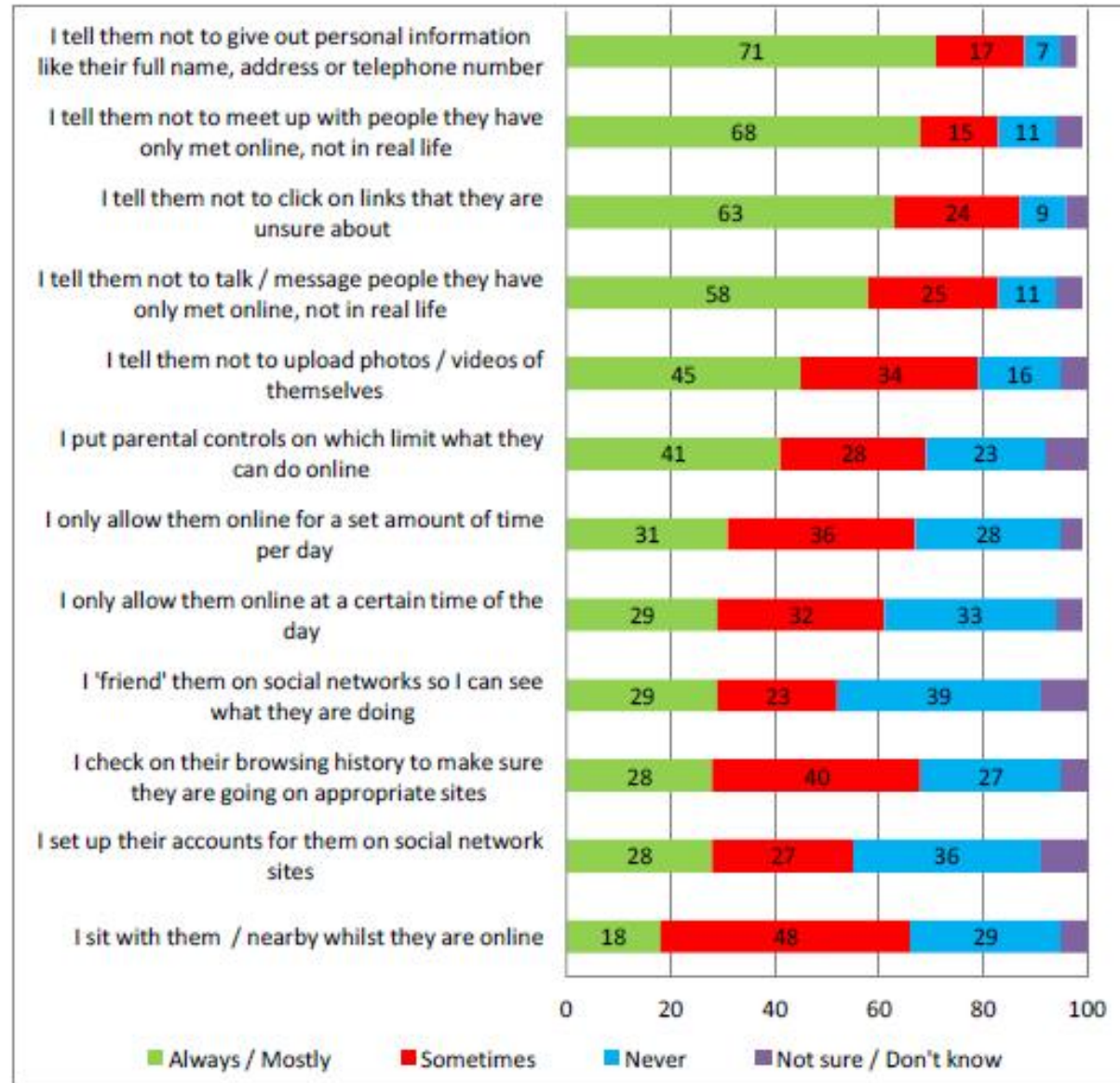- Children as young as 11 post an average of 26 times a day.

Websites and apps used

- Facebook (60%), Instagram (56%) and snapchat (58%) are the most popular social networks
- You tube is the most popular website (83% of children)

- 40% of children have used a "riskier" app.
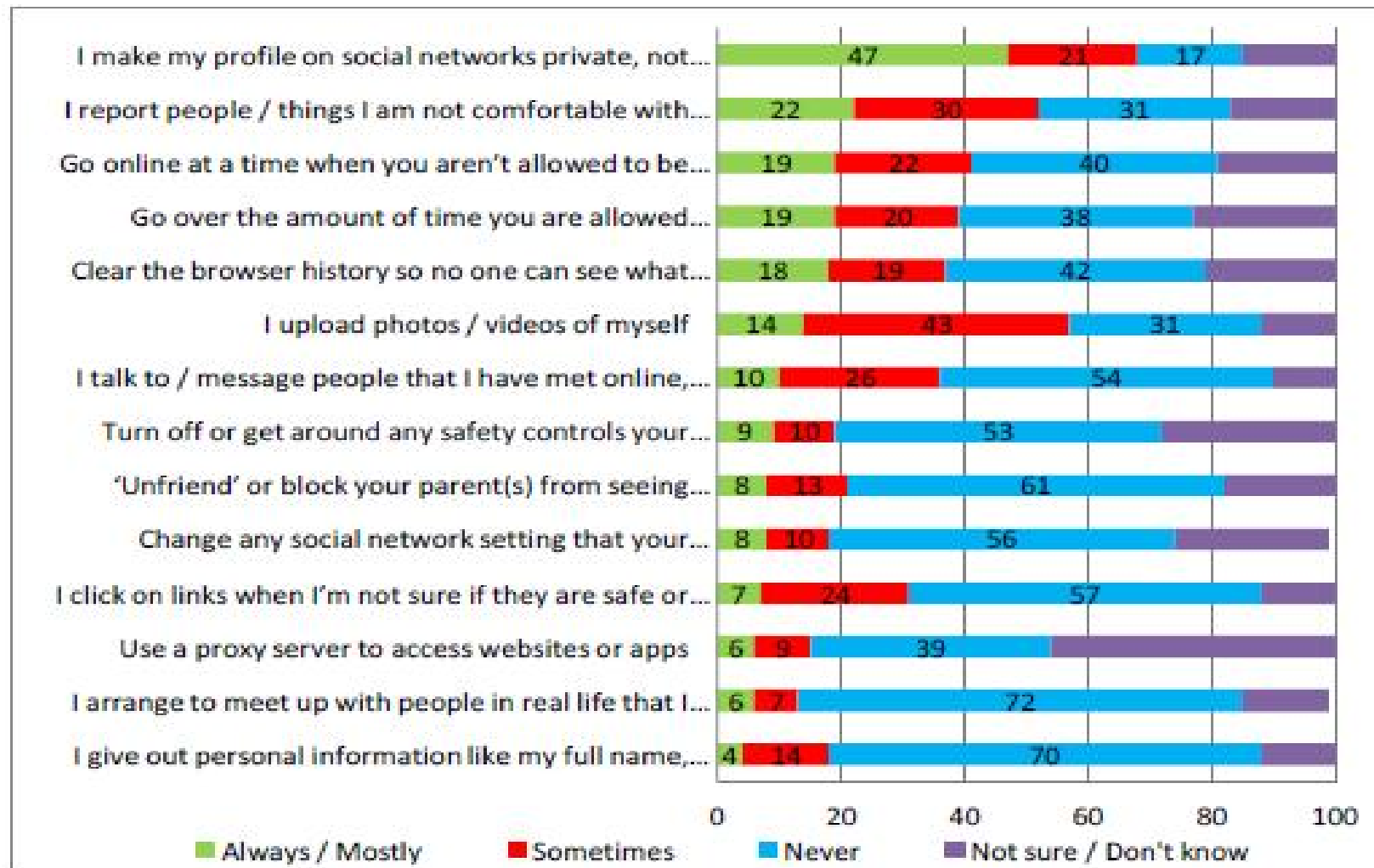- The most popular of these is Kik messenger.
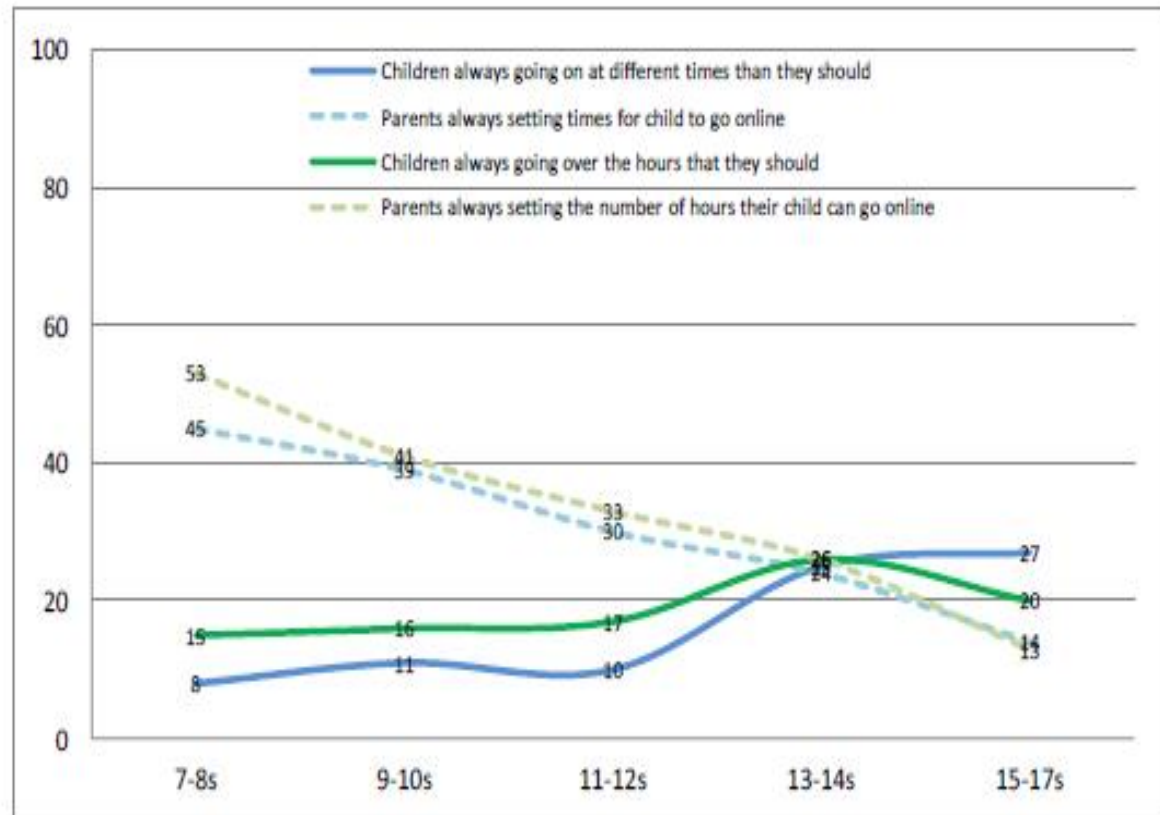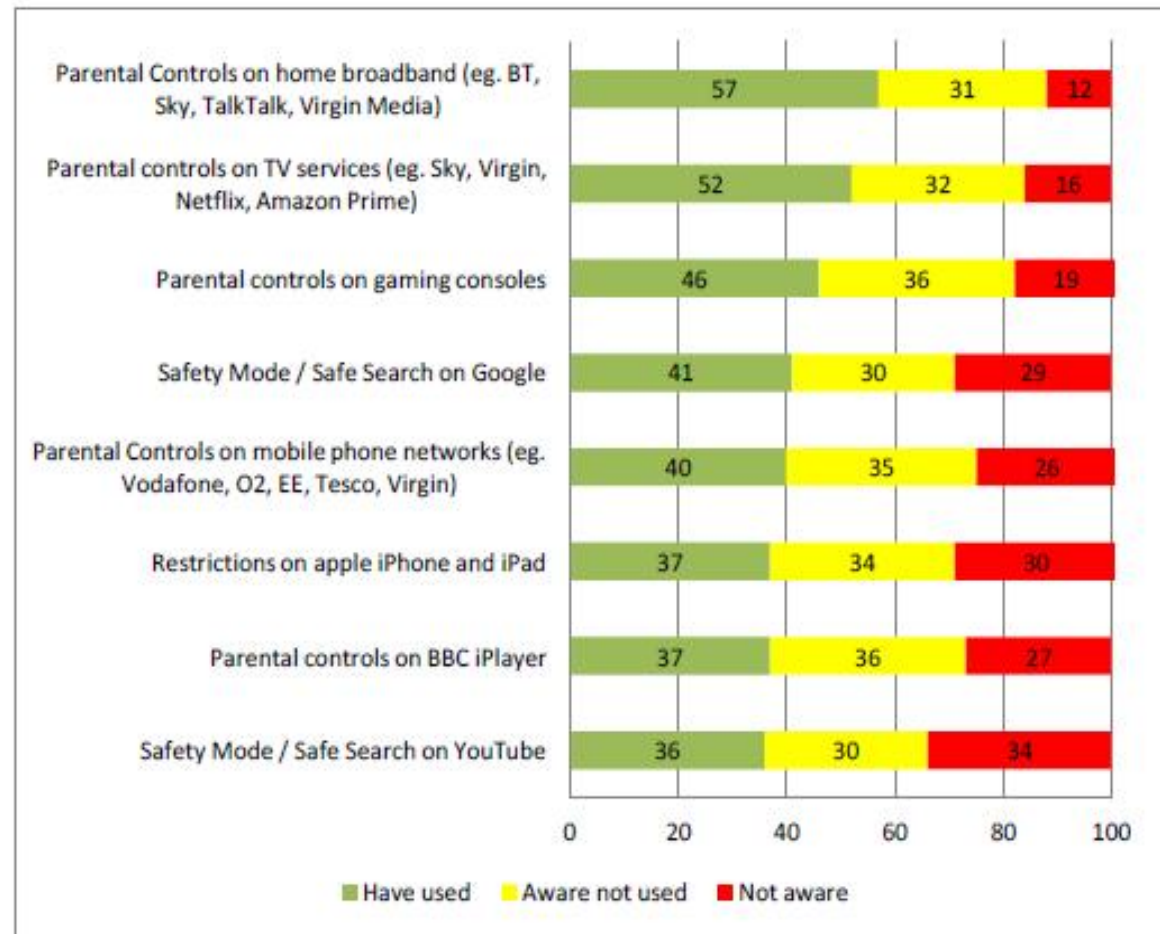
Approaches to keep children safe online

	Always / Mostly	Sometimes	Never	Not sure / Don't know
I tell them not to give out personal information like their full name, address or telephone number	71	17	7	
I tell them not to meet up with people they have only met online, not in real life	68	15	11	
I tell them not to click on links that they are unsure about	63	24	9	
I tell them not to talk / message people they have only met online, not in real life	58	25	11	
I tell them not to upload photos / videos of themselves	45	34	16	
I put parental controls on which limit what they can do online	41	28	23	
I only allow them online for a set amount of time per day	31	36	28	
I only allow them online at a certain time of the day	29	32	33	
I 'friend' them on social networks so I can see what they are doing	29	23	39	
I check on their browsing history to make sure they are going on appropriate sites	28	40	27	
I set up their accounts for them on social network sites	28	27	36	
I sit with them / nearby whilst they are online	18	48	29	

■ Always / Mostly ■ Sometimes ■ Never ■ Not sure / Don't know

What children do online

	0	20	40	60	80	100
I make my profile on social networks private, not...	47		21	17		
I report people / things I am not comfortable with...	22	30		31		
Go online at a time when you aren't allowed to be...	19	22	40			
Go over the amount of time you are allowed...	19	20	38			
Clear the browser history so no one can see what...	18	19	42			
I upload photos / videos of myself	14	43		31		
I talk to / message people that I have met online,...	10	26	54			
Turn off or get around any safety controls your...	9	10	53			
'Unfriend' or block your parent(s) from seeing...	8	13	61			
Change any social network setting that your...	8	10	56			
I click on links when I'm not sure if they are safe or...	7	24	57			
Use a proxy server to access websites or apps	6	9	39			
I arrange to meet up with people in real life that I...	6	7	72			
I give out personal information like my full name,...	4	14	70			

■ Always / Mostly   ■ Sometimes   ■ Never   ■ Not sure / Don't know

How behaviours change with age

- As children get older they are more likely to disregard set times for internet use and time limits.
- Boys are more likely than girls to disobey restrictions.

Parental controls

- Awareness amongst parents is high.
- Around half of parents use parental controls of some sort.

Parental Controls on home broadband (eg. BT, Sky, TalkTalk, Virgin Media) — 57 | 31 | 12

Parental controls on TV services (eg. Sky, Virgin, Netflix, Amazon Prime) — 52 | 32 | 16

Parental controls on gaming consoles — 46 | 36 | 19

Safety Mode / Safe Search on Google — 41 | 30 | 29

Parental Controls on mobile phone networks (eg. Vodafone, O2, EE, Tesco, Virgin) — 40 | 35 | 26

Restrictions on apple iPhone and iPad — 37 | 34 | 30

Parental controls on BBC iPlayer — 37 | 36 | 27

Safety Mode / Safe Search on YouTube — 36 | 30 | 34

0   20   40   60   80   100

■ Have used   ■ Aware not used   ■ Not aware

Cyberbullying

- Children experience more cyberbullying as they move through secondary school
- Children can find it easier to write online than talk face to face.
- This can be people they know; friendship issues, boyfriend / girlfriend issues or social media misunderstanding.
- This can be unknown people, for example through online gaming.

HOW FREQUENTLY DID YOU EXPERIENCE CYBERBULLYING?

(Any bullying that is online or via your mobile phone)

1 - Never	2	3	4	5 - Often	6	7	8	9 - Constantly
35%	15%	10%	7%	10%	6%	6%	4%	7%
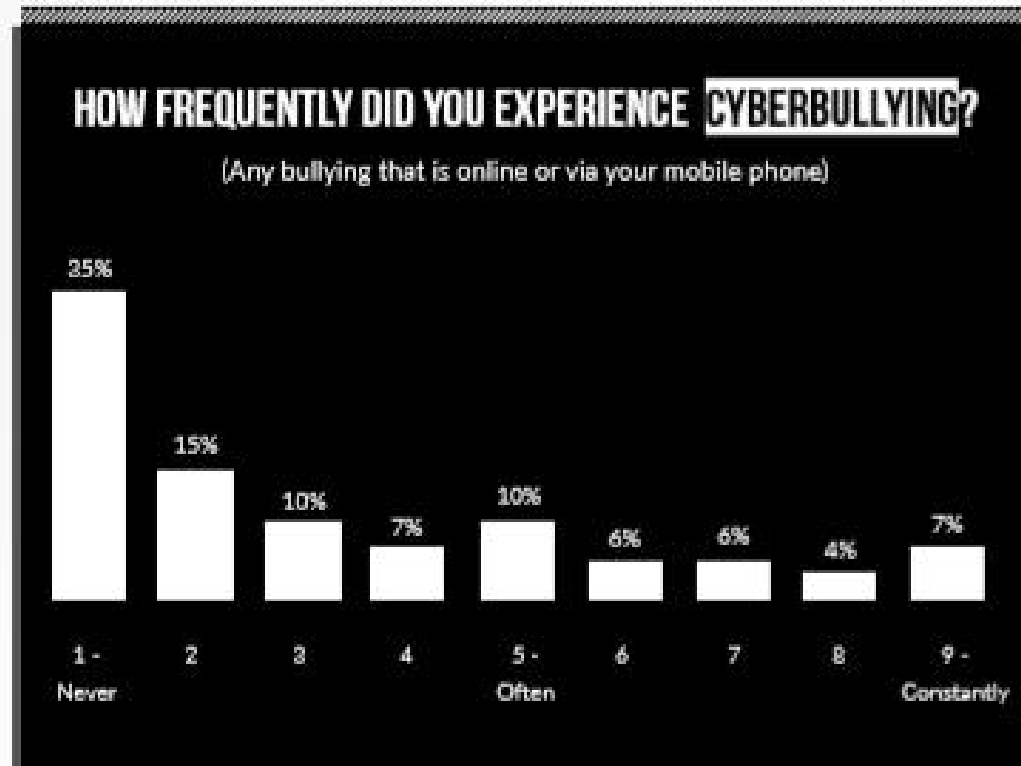
Access to inappropriate content

- 48% of 11-16 year olds have seen pornography online.
- 7% of 11-16 year olds have shared a naked or semi naked image of themselves.
- More boys than girls choose to view pornography.
- Behaviours can include;

developmentally inappropriate use of pornography

sexual harassment

grooming

sending sexual texts, including sexting without images

exposing other children and young people to pornography.

Online grooming 1

- All children can be at risk of sexual exploitation when going online and interacting with strangers, even if they have a supportive home environment.

- What starts as an innocent and harmless chat with a 'friend', can very quickly develop into a dangerous relationship with devastating consequences.

- The word 'grooming' is used to describe the process that abusive adults use to trick a child or young person into believing they are trustworthy so that they can eventually sexually exploit them.

- The different stages of grooming – targeting, friendship forming, loving relationship and abusive relationship – can progress very quickly online and not all stages, such as the loving relationship, may take place.

Online grooming 2

- Grooming is most prevalent for 14-17 year olds. (From the Barnado's online grooming survey 2016)
- Almost half of children groomed online were exploited by more than one perpetrator. This can include instances where children are groomed online, go on to meet the person who groomed them and be sexually exploited by them and others.
- Children were also exploited through the use of technology in other ways. This included sexting, peer exploitation, exchange of films/ photographs, encouragement to self-harm, encouragement to engage in harmful sexual behaviour, and sexual role play through animated profiles or online gaming.

What is illegal?

The following types of content may be classified as illegal:

- footage of real or simulated violence, criminal activity or accidents from video clips, games or films

- sexually explicit content

- images of child sexual abuse

- content that advocates the doing of a terrorist act

- content instructing or promoting crime or violence.

Prohibited actions

- Make prohibited material or permit prohibited material to be made

- Distribute prohibited material

- Have in possession prohibited material with a view of having it distributed or shown

- Publish, or cause to be published, advertisement about distribution of prohibited material

Dealing with offensive material

If you see online content that you think is offensive there are number of easy ways to deal with it:

- close the page straight away, hit control-alt-delete and choose to close the window if the site does not allow you to exit
- use a filter or other tool to block adult content, and use safe search settings in your browser
- report offensive content to the site using their reporting tool
- A chain voicemail message is being sent to students currently containing some nasty consequences if it is not sent onto multiple friends, these have previously been in the form of email and text messages
- talk to someone you trust if you have seen something that has shocked or upset you

Respecting privacy things to think about

- Should I post, copy or send this image? comment or respond? will it hurt, upset others or lead to negative consequences?

- Are my privacy settings set so that I am only sharing information with people I trust?

- Think carefully about the photos you choose to share online; do they give away a lot of information (e.g. a picture of you in your school uniform)? Also keep in mind that photos can be easily copied, changed or shared.

Privacy settings

f facebook

Home	Privacy Shortcuts	Q

Privacy Shortcuts

🔒 **Privacy Checkup**

🌐 Who can see my stuff? ⌄

👥 Who can contact me? ⌄

⊖ How do I stop someone from bothering me? ⌄

See More Settings

y twitter
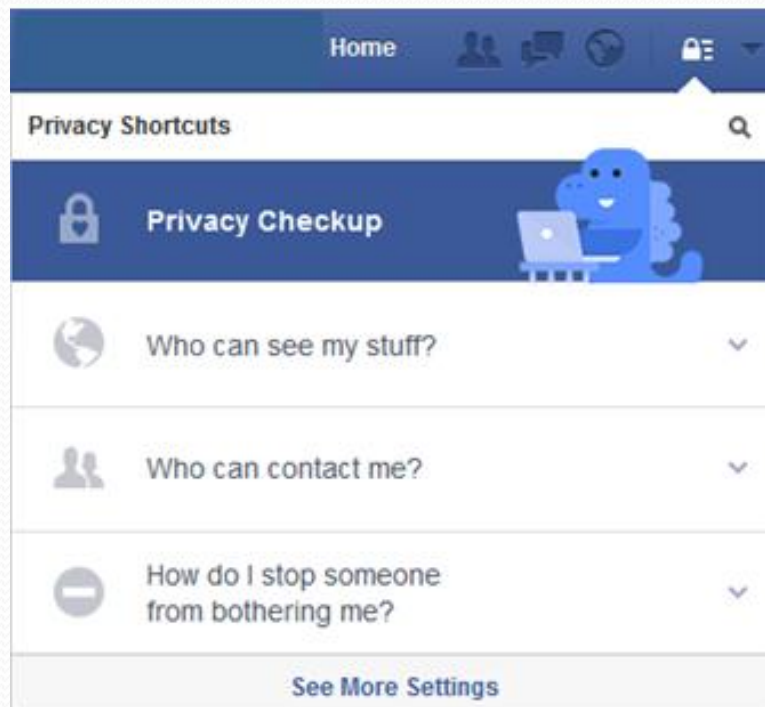
How to protect your Tweets:

1. Go to your Security and privacy settings.

2. Scroll down to the **Tweet privacy** section and check the box next to **Protect my Tweets**.

3. Click the blue **Save** button at the bottom of the page. You will be prompted to enter your password to confirm the change.

Tweet privacy   ☑ Protect my Tweets

If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more.

Privacy settings

Privacy settings

PlayStation Network Privacy settings

You can manage how people contact you on PlayStation Network.

[Privacy Settings] is a feature under PlayStation®Network > [Account Management]. You can set the range for receiving friend requests or messages.

Receive Friend Requests

- Anyone
- Friends of Friends
- No One

Receive Messages

- Anyone
- Friends Only
- No One

Manage your own privacy and online safety on Xbox.com

If you own both an Xbox One and an Xbox 360, we recommend that you manage your settings online.

When you manage settings online, it's easier for you to see which are available on both consoles and which are limited to one console or the other.

For example, content restrictions for Xbox One are managed at the profile level and can be changed online. But on Xbox 360, they are located on the console itself and therefore must be changed on the console.

Where the consoles share the same privacy and security settings, you can make the changes online and apply those changes to both consoles. To manage your privacy and online safety on Xbox.com, follow these steps:

1. Sign in to My Account on Xbox.com.
2. Review and modify the current settings for both the Xbox One and Xbox 360.
3. If a setting is available on both consoles, you can select whether you want it applied to one or both consoles.
4. If a setting is only available on one console, you can apply it only to that console.

Privacy settings
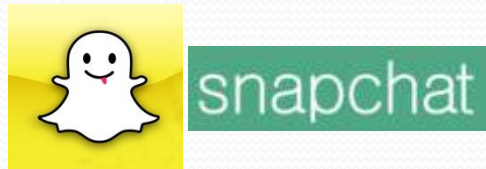
How to Edit Your Privacy Settings

Snapchat has two privacy settings, one for who can send you Snaps and another for who can see your Stories.

For Who Can Send Me Snaps, you have two privacy options: "Everyone" and "My Friends."

For Who Can View My Story, you have three privacy options: "Everyone," "My Friends," and "Custom."
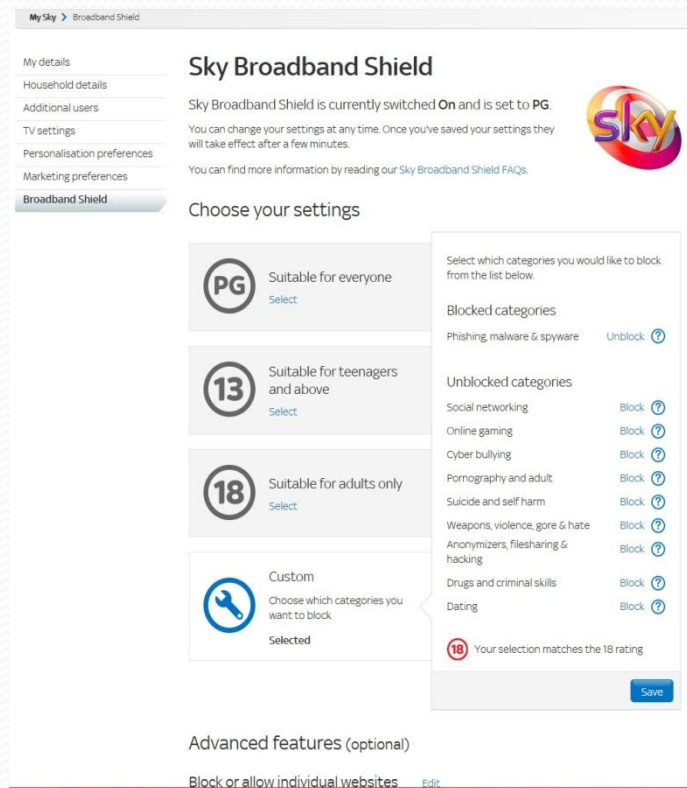
By default, only users you add to your friends list can send you Snaps. If a Snapchatter you haven't added as a friend tries to send you a Snap, you'll receive a notification that they added you, but you will not receive the Snap they sent unless you add them to your friends list.

Turn off location sharing

- [For example; Snapchat 'Ghost Mode'](#)
- When in photo-taking mode, pinch the screen to open your Snap
- Tap the settings cog in the right-hand corner of the screen
- Tap Ghost Mode to switch off location sharing
- Also with KiK, What'sApp and Xbox

Setting parental controls - broadband

Setting parental controls - broadband

- If in doubt contact your broadband provider

Setting parental controls

- Mobile Phone Parental Controls are generally already in place.
- O2, EE, Orange and T-Mobile ask you to either go in-store with an official photo ID, like your passport or driving licence.
- Or you complete a credit card age verification check using an online form to view content.

CONTENT LOCK - CHANGE MY SETTINGS

| EE | Orange | T-Mobile |

What is Content Lock?

Content Lock from EE can help to keep you and your children safe when online.

We have three settings - so you can choose exactly what level of security you'd like. All new accounts have **Moderate** applied by default.

Moderate – With the Moderate setting you have access to social networking sites but not 18-rated content in accordance with a classification framework developed by the BBFC (British Board of Film Classification).

Strict – This is the safe setting for the whole family. This setting filters the same 18-rated content but also includes other content that is not suitable for younger children including un-moderated social networking sites, chat and dating sites

Off - With the **Off** setting you have access to the full internet, including 18-rated content.

If you try to access 18-rated content and Content Lock is not turned off, a blocking page will be displayed and you will need to complete a credit card age verification check using the online form to view the content.

Change or manage your settings

In My Account

You can easily change the Content Lock settings yourself by logging into My Account* – if you haven't registered yet for My Account, get started today.

- Click **Device & usage** in the menu then scroll down to Content Lock to change your settings.
- If you are the account holder you will be able to turn Content Lock off.

Setting parental controls – online media

Any concerns

- Ceop (Child exploitation and online protection) on The School website.
- www.thinkuknow.co.uk
- http://www.parentport.org.uk/
- **Advice for different groups of people**
- http://www.childnet.com/
- https://www.getsafeonline.org/safeguarding-children/
- **Guides for parental controls**

http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/parental-controls

- **Apps guide for parents**

http://www.internetmatters.org/

- **Kidscape**

www.kidscape.co.uk