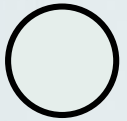


Online Safety Parent Information Workshop – February 2023

This presentation will cover:

- Why is online safety important?
- Online Safety at PTCPS
- Things to be wary of online
- How to set protections, filters and controls
- What you can do for your child
- Where to find help



Why is online safety important?

What happened in an Internet minute - 2020?



Google
4.1m search queries



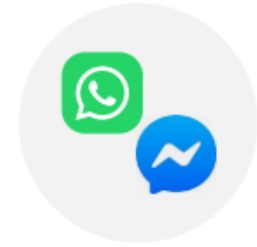
Facebook
1.3m logged in



Instagram
698k scrolls



Twitter
194k tweets



WhatsApp &
FB Messenger
59m messages sent



TikTok
1.4k downloads



Twitch
1.2m views



400k apps
downloaded



1.1m
spent online

Because the internet is incredibly powerful!

internet
matters.org

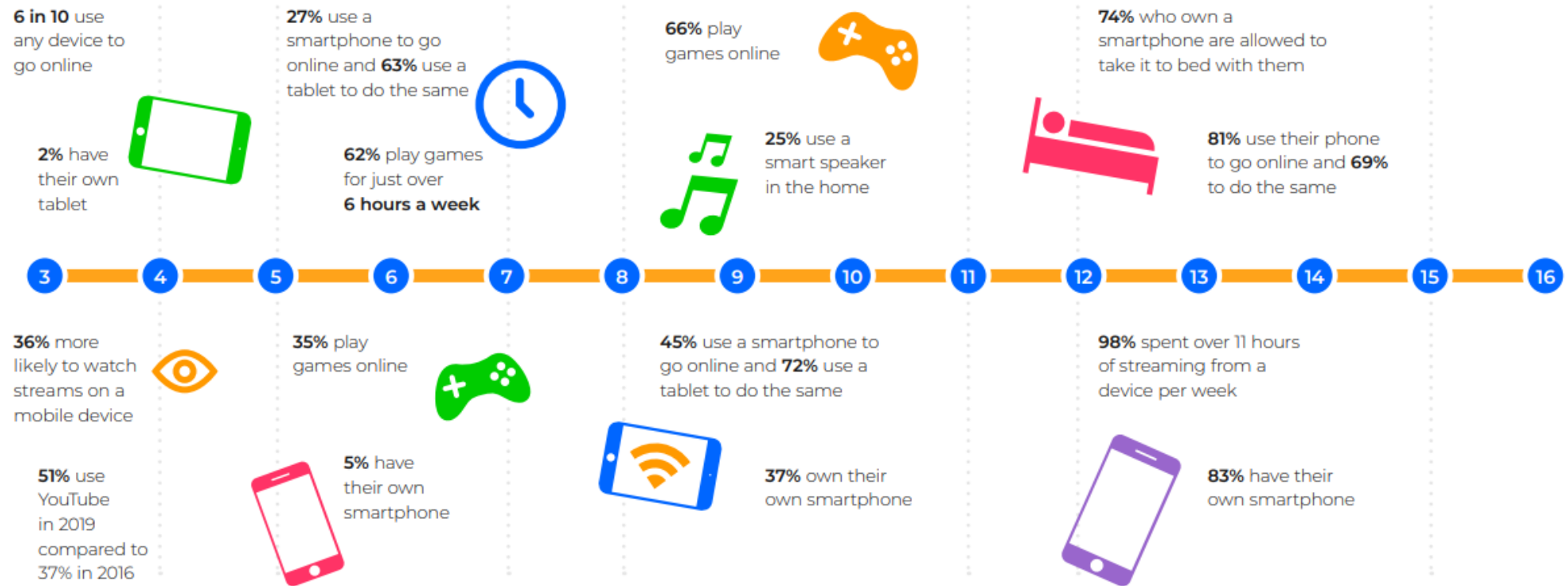
Elm class recently had some teaching from IBM about Cyber Security, using the CyberDay4Girls program. The research team who run the program shared the following statistics:



- Most children under 13 had their own profile on at least one social media app or site; 33% of parents of 5-7s said their child had a profile, and 60% of 8-11s said they had one.
- More than a third of 8-17s who gamed online played with people they didn't know (36%); 16% of 8-17s chatted to people they didn't know, via the messaging/ chat functions in games.

When we look at this alongside Ofcom's 2019 research, we can see that children as young as 3 are using technology and media on a daily basis.

Media usage by age



Reference: Ofcom (2019) https://www.ofcom.org.uk/_data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf

The internet is such a huge part of our lives that we often don't even realise we're using it.





Doorbells, shoes, watches, kettles, fridges, cars, light bulbs, thermostats and washing machines are just some of the everyday items that can be controlled remotely, or by voice, through the internet. Not to mention the entire world of knowledge at our fingertips through our mobile phones, tablets, or AI devices.

It's fantastic, but the potential for children to be involved in foul play, fraud, overuse, inappropriate use and exposure to content which they are too young for is very high.

○
Online safety is important because our children are important!

Risks parents are concerned about

Concerns	% of parents
Encouraging self-harm	62%
Privacy and data collection	50%
Cyberbullying	45%
Radicalisation	41%
Excessive screen time	25%



Reference: Ofcom (2021) https://www.ofcom.org.uk/_data/assets/pdf_file/0025/217825/children-and-parents-media-use-and-attitudes-report-2020-21.pdf

internet matters.org

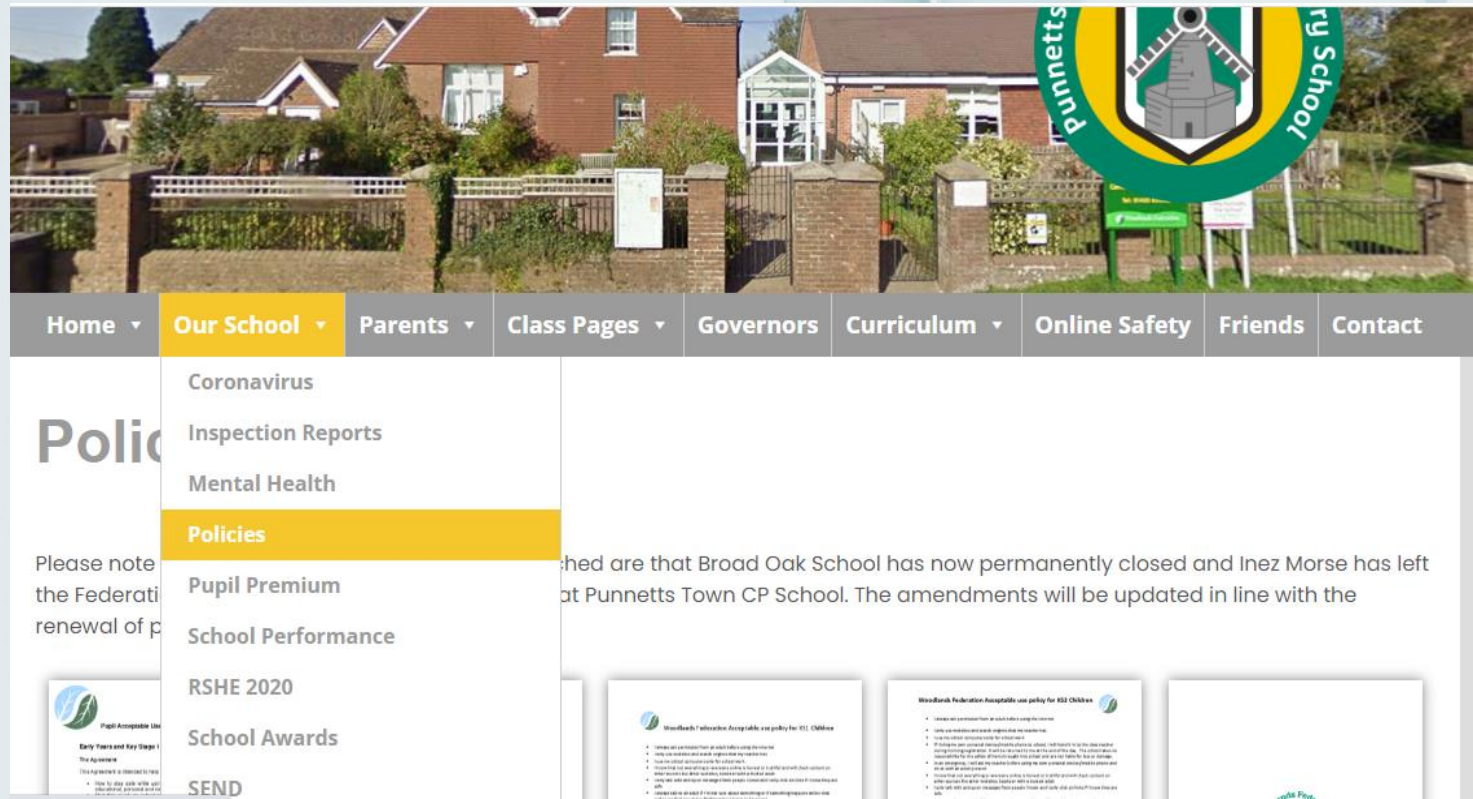
If you want to learn more about Internet Connected Devices, find out what things you have that might have internet access or just check you're using the right settings, this website has lots of helpful advice:

NSPCC Internet Connected Devices

Google and Internet Matters have teamed up to create a Wellbeing Report, which gives parents some key facts about their children's online use, and offers support and advice for keeping children safe online. It makes some valuable but challenging points about our own use of the internet and technology, and how we can foster a positive relationship with devices at home.

Wellbeing Report 2021

What does online safety look like at Punnetts Town Community Primary School?



You will find our Online Safety Policy under the Policies tab on our school website.

We also have some other helpful websites and materials under our Online Safety tab, including links to reporting services like CEOP.



Teachers promote online safety through Computing lessons and other subjects where possible, with the aim of supporting pupils in these areas.

4.5 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to Acceptable Use Policies.
- Understand the importance of good online safety practice out of school, and understand that this policy covers their actions outside of school if related to their membership of the school.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.










Our Computing scheme of work incorporates explicit online safety lessons as well as safety content embedded into other lessons such as data protection within databases, keeping passwords secure when logging on and gaining consent before taking photographs during digital media lessons.

Throughout the year we also organise specific online safety events and teaching from external companies and internally, such as Safer Internet Day each February!



At the beginning of the school year, staff, pupils and parents are asked to read and sign our Acceptable Use policy, which outlines our values and beliefs about staying safe online and suitable use of devices, here at PTCPS.

Each classroom and learning space has these Acceptable Use posters visible too, to support pupils' memory and learning of these important rules. The school council worked with Mrs Golding to produce photos and images to help children's understanding.

 <div>Acceptable Use agreement - KSI</div>		I will be kind to others online when I am sending messages	
I will ask an adult if I want to use the computers / devices and will only use it when they are with me		I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong	
I will only use activities that an adult has told or allowed me to use		I will tell an adult if I see something that upsets me on the screen or if I am worried	
I will keep information about me safe		I know that if I break these rules I might not be allowed to use the computers / devices	
I will not share my password			

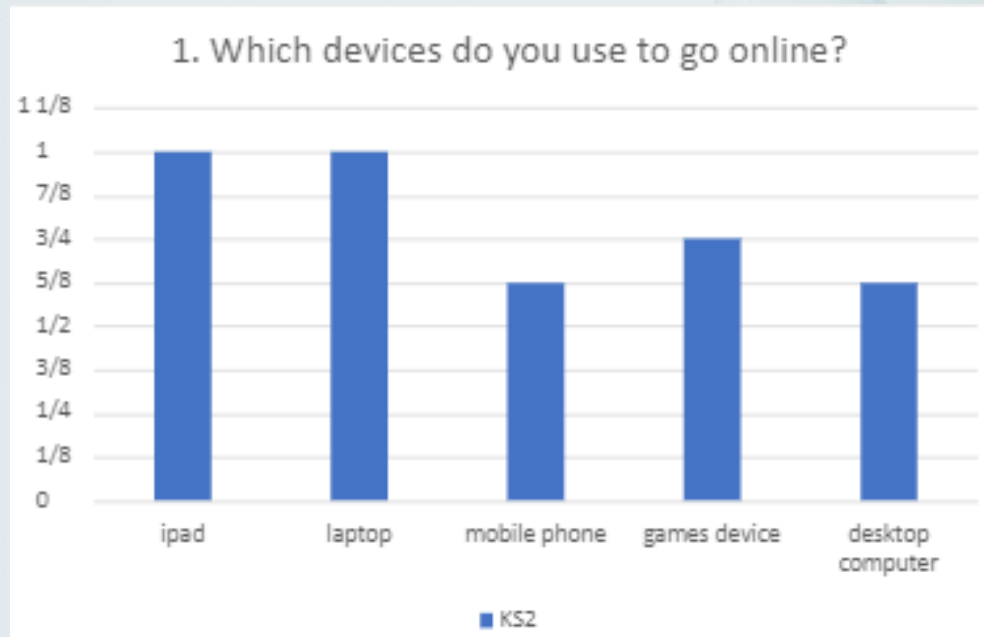
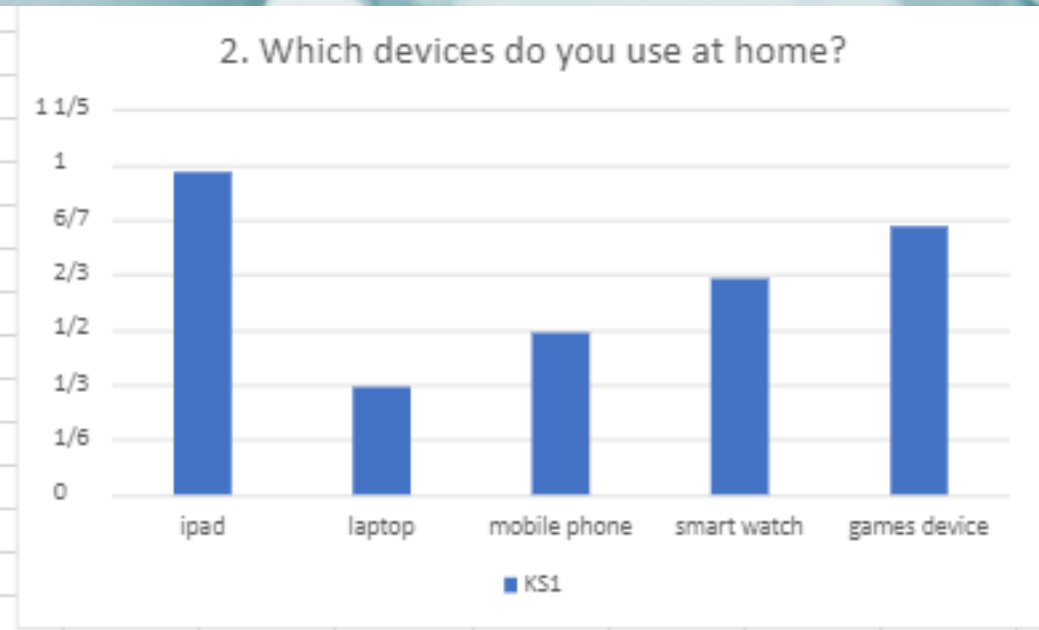
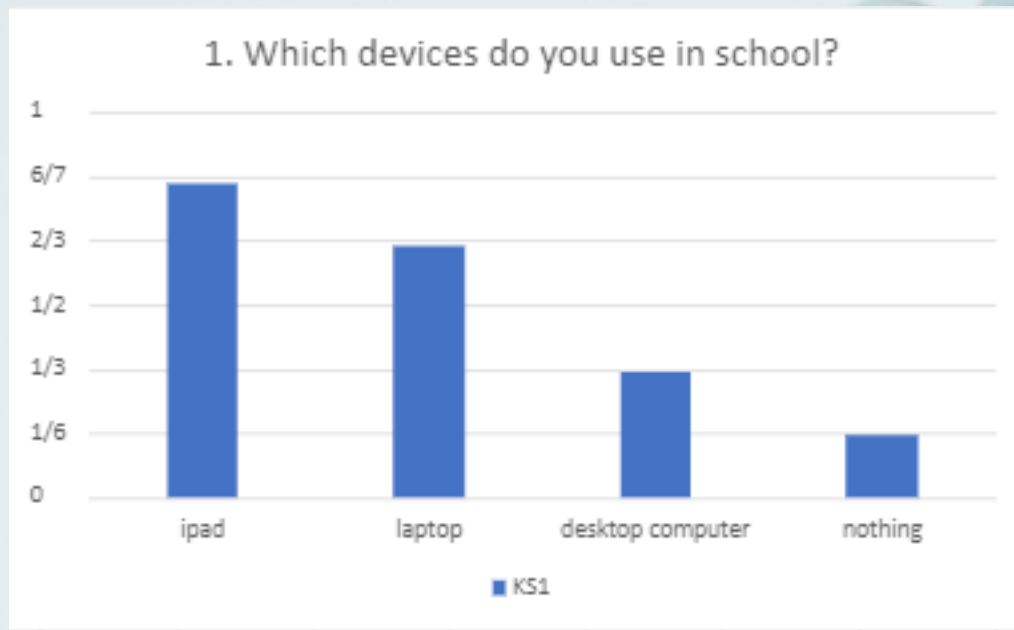


Acceptable Use agreement – KS2

I know that I will be able to use the internet for many different activities and to keep myself and others safe I must use it responsibly	
I will not share my password with anyone, and I will log off when I have finished using the computer or device	
I will protect myself by not telling anyone I meet online any of my personal information. This includes my address, my telephone number, my name	<p>What is your address?</p> <p>I won't tell you that.</p> <p>What about your phone number?</p> <p>I won't tell you that either.</p>
I will not send a picture of myself without permission from a teacher or other adult	
I will not arrange to meet anyone I have met online alone in person without talking to a trusted adult	

I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps	
I know that posting anonymous messages or pretending to be someone else is not allowed	
I know that information on the internet may not be reliable and it sometimes needs checking so I will not download any material from the internet unless I have permission	
I know that information on the internet may not be reliable and it sometimes needs checking so I will not download any material from the internet unless I have permission	
I know that memory sticks/CDs from outside of the school may carry viruses so I will always give them to my teacher so they can be checked before opening them	
I know that I am not allowed on personal email, social networking sites or instant messaging whilst at school	

I know that all devices/computers and systems at school are monitored, including when I am using them at home	
I will be polite and sensible when I message people online	
I will not be rude or hurt someone's feelings online	
I will not look for bad language, inappropriate images or violent or unsuitable games, and if I accidentally come across any of these I will report it to a teacher or adult, or a parent/carer at home	
If I get unkind, rude, or bullying emails or messages, I will report them to a teacher/adult. I will not delete them, I will show them to the adult	



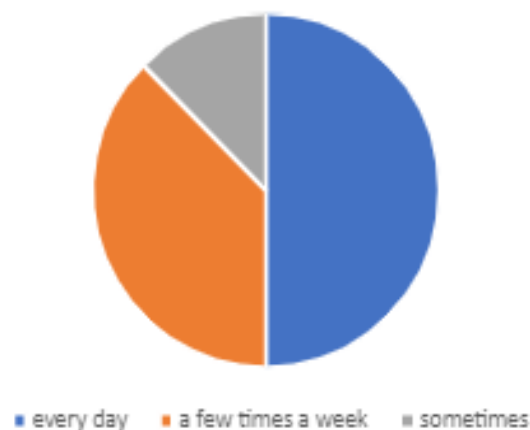
Mrs Golding carried out an online safety questionnaire with a few pupils from both Dallington and Punnetts Town. In each school, 6 Key Stage 1 and 8 Key Stage 2 children completed the questionnaire. Here are some of the results.

3. How often do you go on the internet or your device?



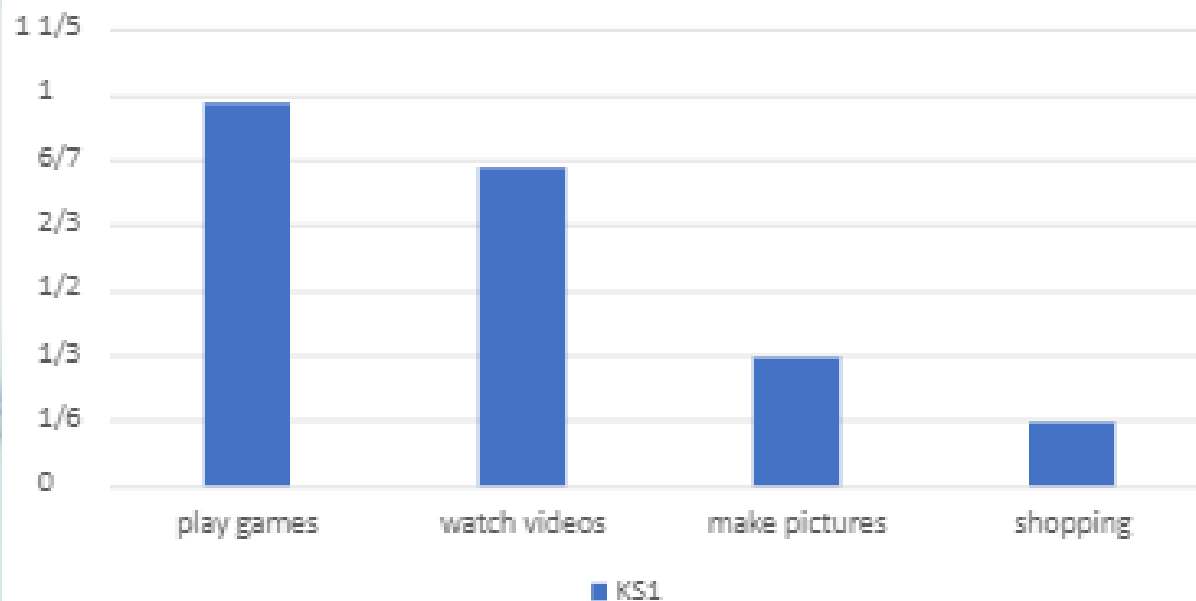
KS1

2. How often do you go on the internet or your device?

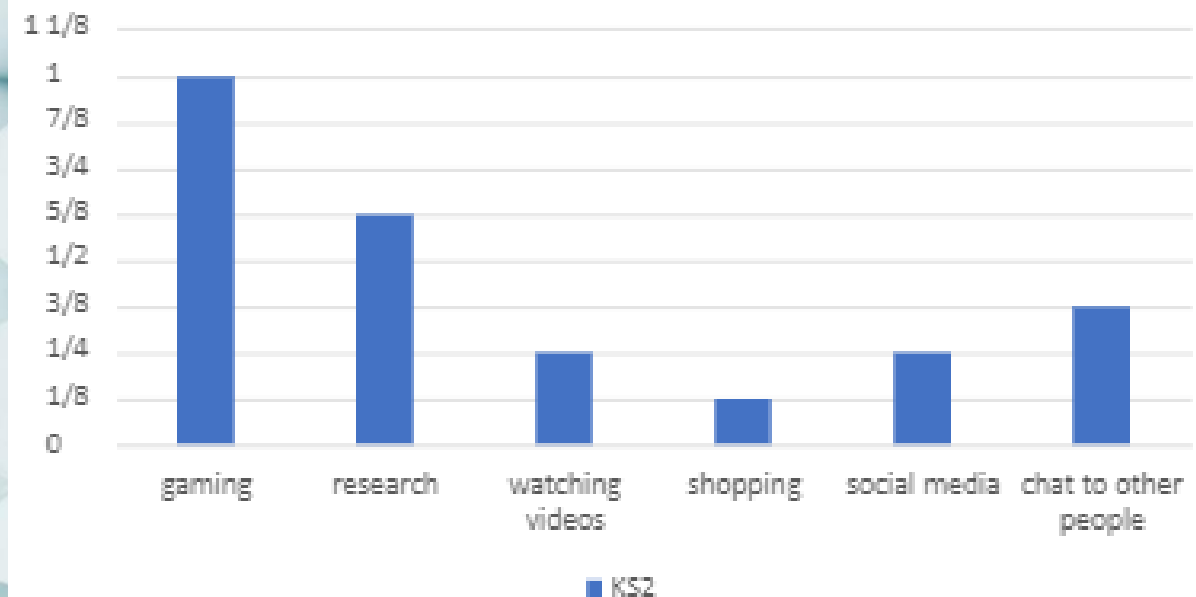


KS2

4. What do you do when you go online?



3. What do you do when you go online?



5. Do you feel safe when you are online at home?



KS1

■ yes ■ sometimes

6. Does someone help you at home when you are online?



KS1

■ yes ■ no ■ sometimes

7. Do your parents or carers set online safety rules?



KS2

■ yes ■ no

5. Do you feel safe when you are online at home?



KS2

■ yes ■ no

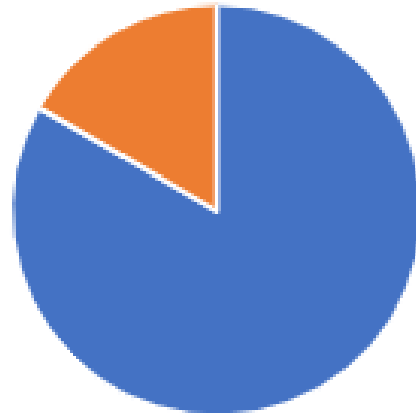
6. Do your parents or carers talk to you about online safety?



KS2

■ yes ■ no ■ sometimes

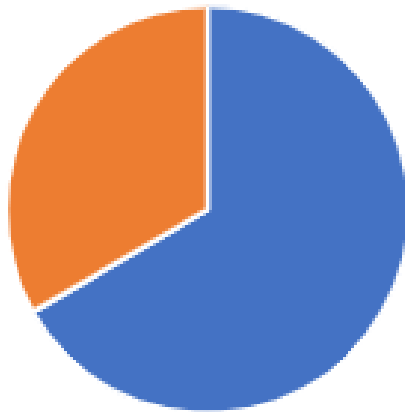
8. Have you ever been upset by something online?



■ no ■ yes

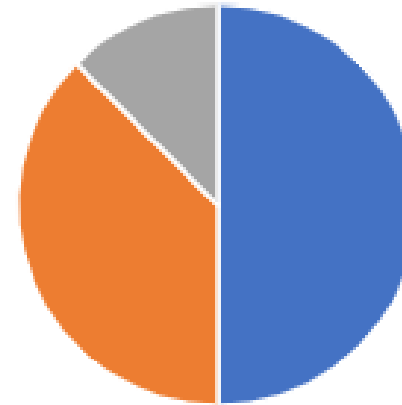
KS1

9. If you are upset by something online, do you know what to do?



■ yes ■ no

12. Do you know how to report and block upsetting things online?



■ yes ■ no ■ sometimes

KS2

The most popular apps the children said they use were:

- YouTube (one child named YouTube Kids)
- Roblox
- Google (two children named Google SafeSearch)
- Minecraft
- WhatsApp
- Snapchat
- TikTok

At Punnetts Town, we recognise the valuable contribution that parents make to their children's learning and life experience. We always want to work closely with you to make sure that your child is happy, safe and learning, across all areas of the curriculum. That extends to online safety, and it is important that we all work together to keep our children safe wherever they might be accessing the internet, and whatever they may be using it for. Parents' roles are included in our Online Safety policy.

4.6 It is the responsibility of parents and carers to:

- Read the Acceptable Use Policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the Acceptable Use Policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

What can parents do to help children stay safe online?

1. Know what the risks are
2. Set protections, controls and filters
3. Talk to your child about online safety
4. Know where to go for help



1. What are the risks?

There are three main areas of concern and consideration when children or vulnerable people use the internet. These are:

- **Content** What children might find on the internet. This could be in response to a direct search, or could be involuntarily found through pop ups, unfiltered links or passed on from a friend/online contact
- **Contact** Who children speak to online. This could be through email or online messaging apps where you speak to someone you know by entering their contact details. However, many gaming sites and apps have a chat function where users can talk to other users, including those they don't know
- **Conduct** How children and other users behave online, including how they communicate with each other and their approach to internet use

2. Set protections, controls and filters

Most of the dangers within the three 'C's can be mitigated by putting measures in place.

Content can be filtered so that inappropriate language or search results are not shown. However, filters are never 100% successful, so there may be things that slip through the net. Some apps cleverly avoid filters and show users content related to self-harm or suicide, extremism or racist beliefs, violent or distressing content, pornographic images or videos, edited videos and images or fake news and hoaxes. This is all unsuitable content for our children and vulnerable people, and we need to be aware that there is always a risk of children being exposed to these dangers, even when we use filters. The NSPCC offers some helpful advice and support lines for children who have been exposed to inappropriate content, and their parents (link below). Many public places now have 'friendly wifi' which also filters search results and protects children online – see link for more information and to see the logo to look for.

[NSPCC Inappropriate content](#)

[Friendly Wifi](#)

2. Set protections, controls and filters

Many home WiFi networks allow users to create different profiles or settings for their children too.

Follow the link below to see instructions for some of the main internet providers and learn how to set up these measures in your home.

Parental Controls Internet Provider

Another control parents can put in place is to enable Google 'SafeSearch' on devices which their children have access to. Use the guide to learn how to enable and disable this.

SafeSearch

Internet Matters have a fantastic resource which allows parents to see instructions for enabling parental control settings on various game consoles, social media apps and smartphones and devices. Follow the link to use it.

Parental Controls

Google's 'Family Link' app is brilliant. It allows parents to control their children's device and internet use, setting time limits, protecting privacy and seeing location. Consider downloading it for your family.

Family Link app

2. Set protections, controls and filters

Contact can be limited and controlled from parent devices. Many gaming apps have a chat function, which can be disabled. Check the settings of each app and disable anything you are not comfortable with for your child. Some settings also seem to enable a feature which replaces bad or inappropriate language with hash tags so that children can be protected and keep their personal information safe. At PTCPS we teach children to NEVER agree to meet with somebody they have met online, and to protect their personal information (like full name, age, address, phone number, school, passwords etc.)

Most social media apps have a recommended age of 13, so parents should not let their children set up an account, and should not set one up for them, before this. This will help to protect vulnerable younger children from some more mature content they might find and prevent children from making contact with people they do not know online.

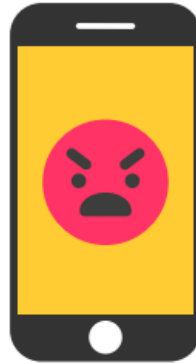
Many parents and children worry about Cyberbullying, which has many other related terms.

Cyberbullying terms

Cyberstalking

Outing

Harassment



Dissing

Flaming

Griefing

Masquerading

Frapping

Roasting

Exclusion

Trolling

Catfishing

Spotting the signs

1 in 10

parents are unaware
their child has
been bullied

54%

of parents
worry about
Cyberbullying

Why children might not report being bullied:

- embarrassment (39%)
- being labelled a snitch (38%)
- fear it will get worse (38%)
- worry they won't be taken seriously (30%)
- nothing was done about reported bullying in the past (23%)



The main way to ensure that your child **conducts** themselves appropriately online is to show them what this looks like, by modelling good online behaviour yourself. Internet Matters suggests these key rules:

Have great internet manners



1. Treat others as you would like to be treated



2. If you wouldn't say it to someone in person don't say it online



3. People can't see your body language, facial expressions or hear the tone of your voice online – so don't over-use icons and punctuation to convey meaning



4. Don't make a situation worse by provoking people even more



5. Don't start rumours or spread gossip about someone online



6. Don't make fun of someone in an online chat



7. Post things that will inspire and motivate people in a positive way



8. Make sure you don't create a negative environment in an online world or game through name calling



9. Include people in online games and social forums, and don't intentionally leave people out.



10. You can't retrieve material once it's sent or posted online so if it might embarrass you or someone, don't put it online



11. Respect other people's privacy



12. Respect other people's time and bandwidth by avoiding posting too much information

Internet
matters.org

School and home can work together to teach children the following things about keeping a safe social media profile:



Use a strong password



Use an alias and avoid personal pictures



Don't include date of birth and other personal information



Show your child how to block and report



Change settings to private



Consider the minimum age



Don't accept friend requests from strangers



Switch off location services



Tell them to think before they post

In situations where your child unfortunately does experience some form of Cyberbullying, there are places to seek help and support for your child and for yourself.

The do's



Block



Report



Keep the
evidence



Know when to
take it further

Children can speak to someone at Childline about their experience.

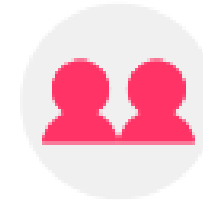
The dont's



Retaliate



Stop them
going online



Deal with
it alone








Stop when the
bullying stops

CEOP Thinkuknow

Anybody can report an issue on CEOP, and the 'Thinkuknow' website gives tips on how to block and report on different social media apps.


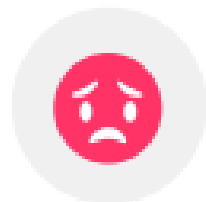

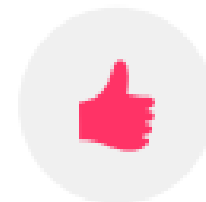

If you discover that your child has been participating in inappropriate conduct online, or acted as a bully, Internet Matters gives this advice:

The do's

-  Find out why
-  Talk it through
-  Stay calm
-  Teach by example
-  Learn from it

InternetMatters.org

The don't's

-  Ignore it
-  Get upset
-  Be judgmental
-  Condone it
-  Take away their devices

InternetMatters.org

The NSPCC has this page dedicated to finding out more about cyberbullying and how to support your child: [NSPCC Cyberbullying](https://www.nspcc.org.uk/keeping-children-safe/online-safety/cyberbullying/)

3. Talk to your child

Explain to your child every action you are taking to protect them. They may not like or agree with some of the steps you take, but if they understand why you are doing it, they will feel loved and know they can talk to you if and when a problem arises.

Choices you make might be controversial or unpopular, but it is important that parents are in control of their children's internet and device usage, and don't compromise what they want for their child just because they say, "all my friends are doing it!"

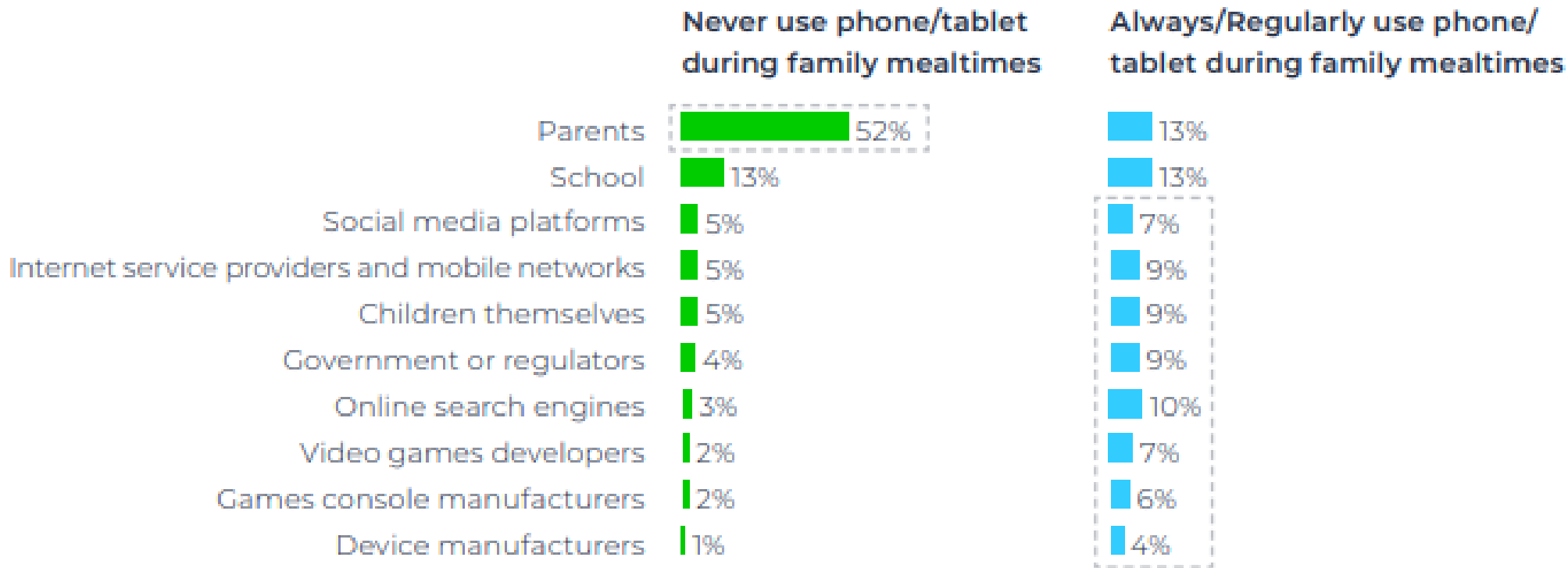


3. Talk to your child

Setting a good example is also important when talking to your child about online safety. Children are most likely to imitate the behaviour around them, so if parents are responsible technology users, they are more likely to be too!

Remember, what you do matters!

Parent views of who is the most responsible for supporting their children to have positive experiences online



Base: Total sample parents of children aged 4-16 (n=2010); 'use my phone or tablet during mealtimes with the family' – Never (n=774), Always/Regularly (n=647)
Dashed lines indicate significantly higher among this group

4. Know where to go for help

You can find lots of information and parent support, including age guides for different social media and gaming apps on the Internet Matters website, by following this link:

[Age Guides, Parent Packs and Resources](#)

There are some social networks which have been designed for, and by, children in order to add a level of protection and to enable those under 13 to connect with their friends online safely. See the list here:

[Social Networks for Kids](#)

You can read more about how to play online games here; the potential risks involved and tips for keeping your child safe.

[NSPCC Online games](#)

National Centre for Cyber Security tips for being Cyber Aware:

<https://www.ncsc.gov.uk/section/information-for/individuals-families>

Cyber Aware and staying secure online

From banking to shopping, and streaming to social media, people are spending more time than ever online. Cyber Aware is the government's advice on how to stay secure online.

[Visit Cyber Aware](#)

As well as our six Cyber Aware actions, the NCSC has provided further guidance for those looking to stay secure online.

- Use a strong and separate password for your email +
- Install the latest software and app updates +
- Turn on 2-Step Verification (2SV) +
- Password managers: using browsers and apps to safely store your passwords +
- Backing up your data +
- Three random words +

Thank you very much for reading this presentation.

Please do get in touch with the school office or with Mrs Golding (rgolding@punnettstown.e-sussex.sch.uk) if you have any questions or would like to discuss any of this information further.

I hope you find it helpful, and that you are able to use some of this information to help keep your children safe online.

