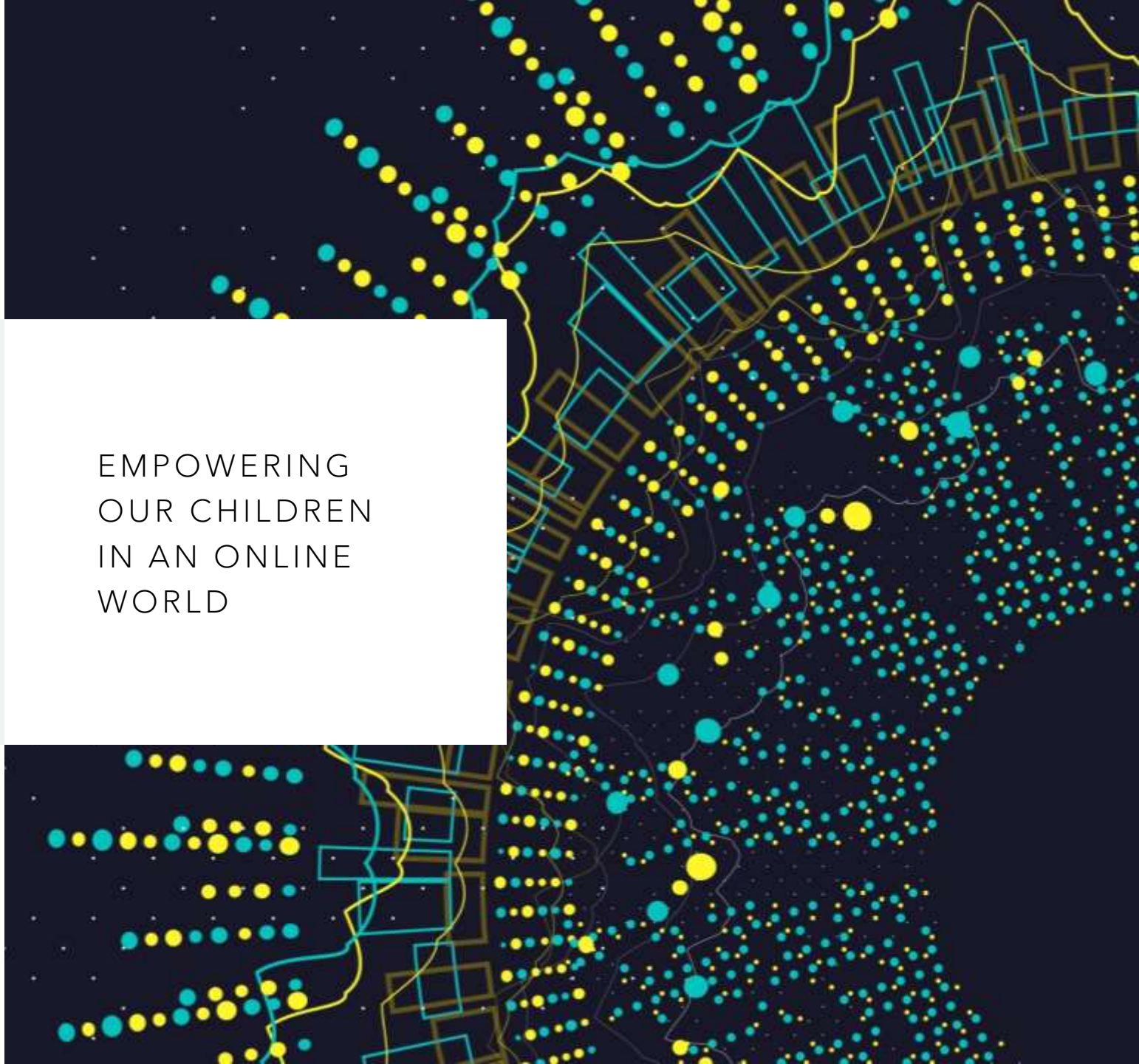
Digital Wellbeing

EMPOWERING OUR CHILDREN IN AN ONLINE WORLD

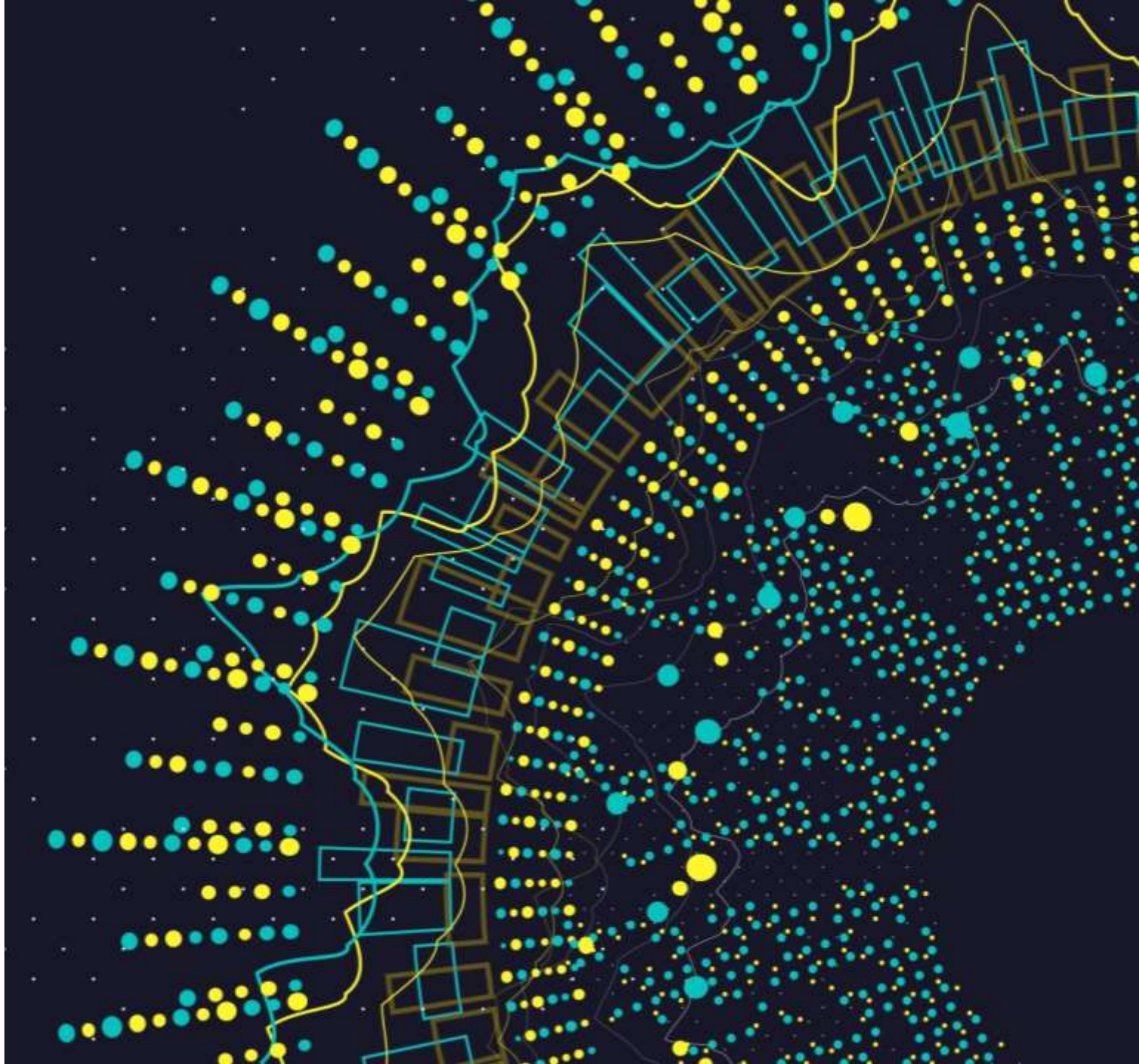


About Me

- Dad to Ed and Hazel

- Security Architect

- Technology Enthusiast

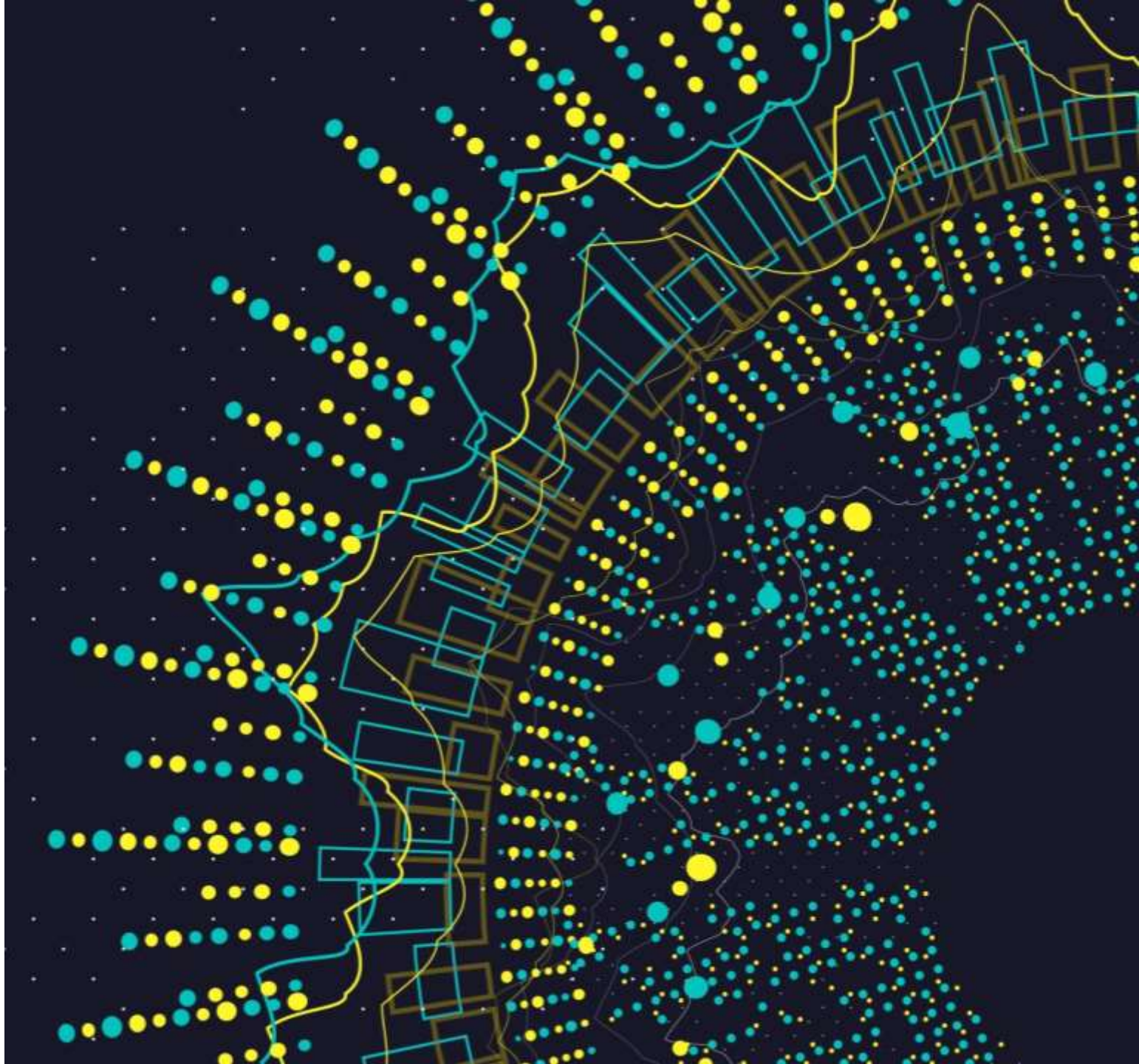


Agenda

I have structured this session on a threat modelling exercise, which is organised into 3 parts:

1. What are our children doing?
2. What can go wrong?
3. What can we do about it?

This is a casual session where we can all share our thoughts, ideas and experiences, so don't be shy!



What are our children doing online?

WHAT IS THE DIGITAL WORLD LIKE TO THEM?

Dad, the thing is…

You don’t understand what things are like for us… When you were our age, the internet wasn’t everywhere!

Edward Larby 2023

What are our children doing online?

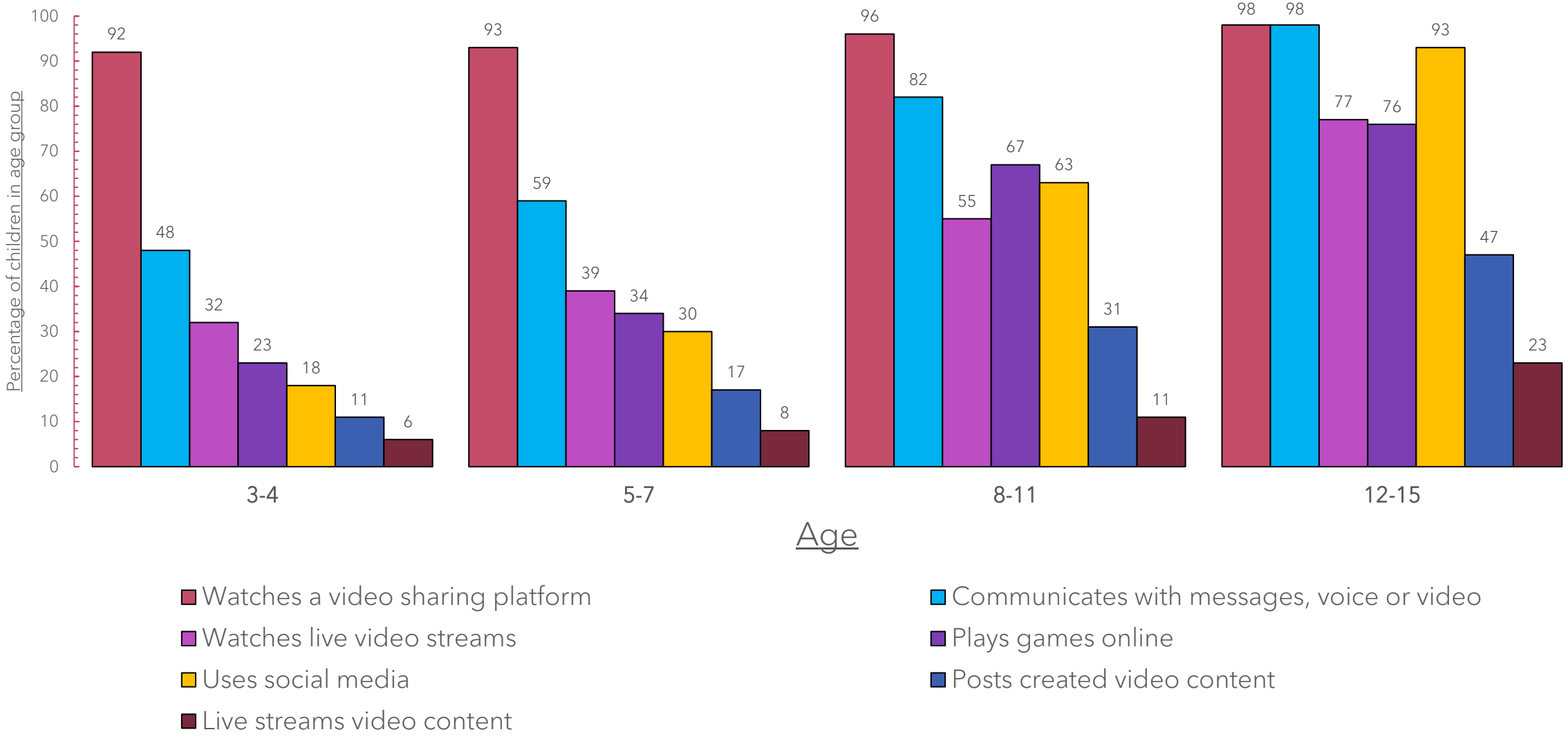
- School work and study
- Learning about the world and current affairs
- Creating
- Consuming (video, audio, literature)
- Playing games
- Visiting virtual worlds
- Social networking
- Communicating with friends and family
- Shopping and browsing
- Etc……..

The online ecosystem is huge

HOW CAN WE, AS PARENTS, DIFFERENTIATE GOOD FROM BAD?

Online activity by age

National figures from Ofcom

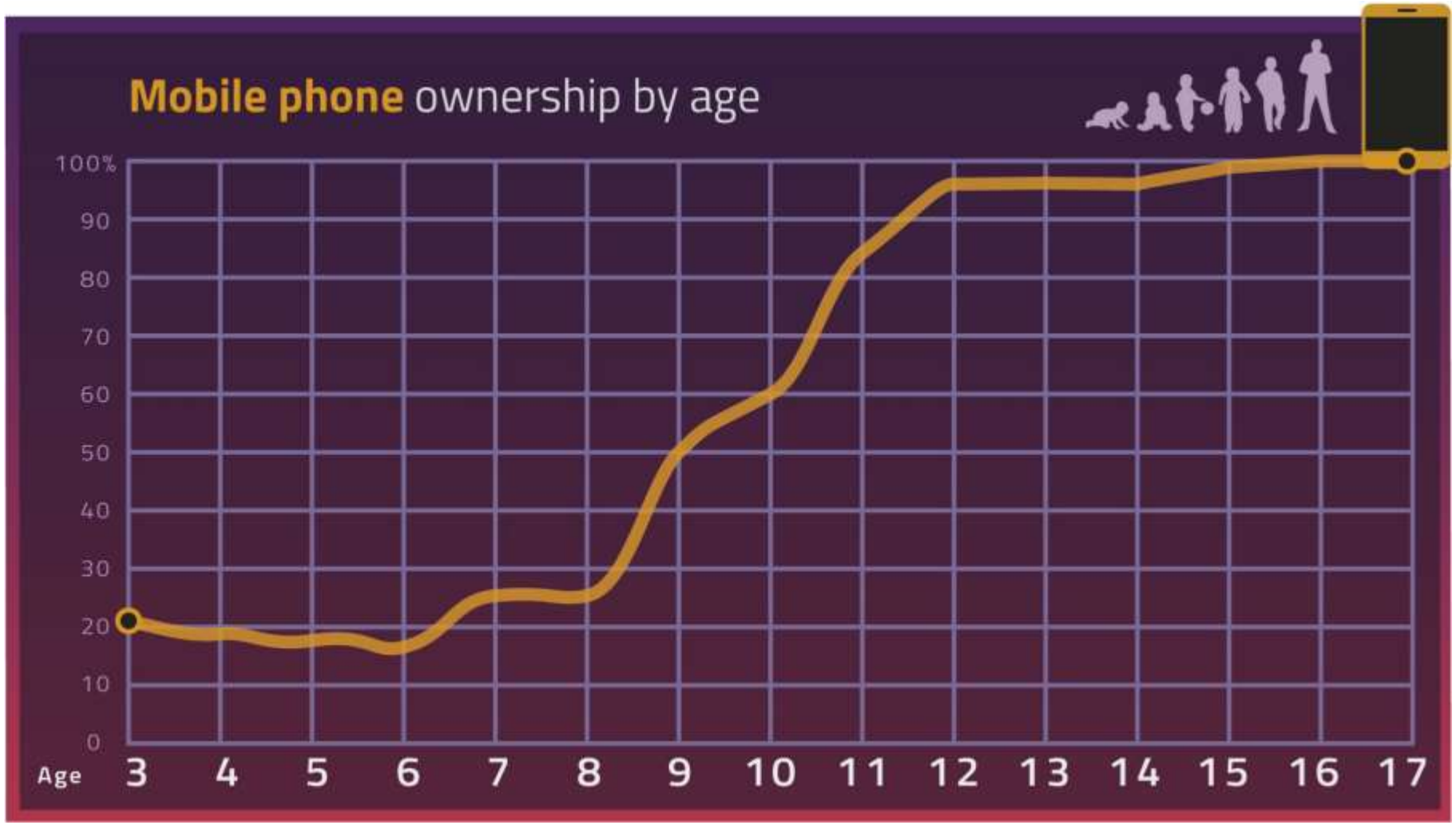


Home is where the hardware is…

(For a while anyway)

Mobile phone ownership

National figures from Ofcom



Technology and Culture

At age 8, average time spent on playing moves from being mostly traditional to mostly digital

* Children and parents: media use and attitudes report 2023

What can go wrong

AND HOW DO WE KNOW?

Communicating

A lot of online activity is built around communication and interaction. This can be positive, but also carries risks

- Casual group communication can be unfamiliar. Children sometime don't consider the whole audience and have private conversations in public channels
- Lack of facial expression, body language and tone can make interpretation of text-based chat difficult
- Social pressure for children to join large groups
- Sense of anonymity and automatically deleting messages can encourage negative behaviours including hurtful communications and bullying

Cyberbullying and online victimisation

NetNanny reports that 43% of children have been a victim of cyberbullying and of those, 58% have not reported it to parents, school or any other authority

Impacts of cyberbullying can include:

- Mental health issues
- Increased stress and anxiety
- Depression
- Violent responses
- Low self-esteem

Cyberbullying can also have a long-lasting emotional impact, even if the bullying has stopped.

Cyberbullying and online victimisation

Signs of cyberbullying can include:

- Nervousness or reluctance around going to school or socialising
- Turning off or hiding devices when you enter room
- Spending long hours on online, especially at night
- Avoiding talking about online activities
- Anger or frustration after online activities
- Anger when denied screen time

Perception is as important as intent. Children do not have the same social filters as adults and without cues from body language and tone, they may not interpret messages as intended or realise they could be causing upset.

Nasty or hurtful experiences

% of children experiencing someone being nasty or hurtful to them via these means

	Face-to-face	Any comms technology	By text or messaging app	On social media sites/apps	In online games	Through phone calls	Through other sites/apps	Through video calls
Total	20%	29%	20%	15%	11%	4%	3%	2%
8-11	18%	20%	10%	6%	10%	1%	3%	1%
12-15	21%	35%	25%	21%	11%	4%	3%	2%
16-17	21%	37%	28%	24%	13%	8%	4%	3%

Managing Privacy

What data does social media (and other apps) collect?

- Anything you add to your profile. Name, email address, phone numbers, likes, friends, communities, inferred information from posted content.
- Location data – Where you live, routes you travel, people you associate with, where you work or go to school, businesses you use, patterns of life
- Interaction data – phone calls, text messages, contacts, hashtags, friends, likes, groups, app use, length of engagements
- Biometric signatures – facial recognition, fingerprint, keyboard rhythms.
- Web usage – Browser history, cookie data, web use monitoring

Many app and platform age limits are due to laws restricting collection of personal data from children

Privacy - Digital Footprint

Your digital footprint is the sum total of all information relating to you that exists about you online.

- Digital footprint have 2 components active and passive
- Digital footprint can paint a very detailed picture of a person, which can be positive or negative
- Some content may be embarrassing or used for bullying, and it is very easy to lose control of this
- Larger, more detailed footprint increases risk of identity theft
- Sharenting – parents or carers publishing photos, videos, stories and personal details of their children online

Location Data

- Most mobile phones ‘leak’ location data
- Funding model for many ‘free’ apps
- Market is global and effectively unregulated
- Location data is collected by data brokers, who make data inferences
- Datasets are incredibly cheap. Population level datasets are < £1000
- Example of data:
  - Identifying school children
  - Routes they walk at what times
  - Where they live
  - Where their parents live and patterns of life
  - Who their friends are
  - Personal details – visits to doctors etc

Gaming

- Check Pan European Game Information (PEGI) rating of games.
  - Age ratings for the same game can vary between countries
  - PEGI rating cover game content, not behaviour of people online
- Games do often have feature and content management, and parental controls
- Voice or text chat in games can be inappropriate, especially in games with mixed age groups. Voice chat can be hostile and used for cyberbullying
- Online communities can be hostile to outsiders or newcomers
- ‘Friend’ systems can be used to manage interactions, but if not managed can be used to perpetuate cyberbullying

Xbox, Playstation and Switch support family and child accounts. PC gaming is more diverse, but major platforms have similar controls.

Roblox

Roblox has the following parental controls:

- Content can be set to ‘all ages’, 9+, 13+ or 17+
- Communication can be disabled or limited
- Time limits can be specified
- In-game purchases can be limited or disabled
- Parental controls can be pin protected

This can be managed on the child’s device, or in the child’s account.

To manage a child’s account, it must have been created as a child’s account and configured with the appropriate age.

Gaming and screen addiction

Some young people can find it difficult to balance online activity with the rest of life. This can leave a young person feeling low or depressed, anxious, angry or isolated.

<u>Signs of addiction to look out for:</u>

- They feel regularly exhausted and disengaged
- They're struggling to concentrate at school
- They prioritise gaming and screentime over important daily activities like sleeping, eating, homework and household job.
- They're mainly socialising online and finding in-person interactions difficult to manage or enjoy
- They no longer keep up with other interests they used to enjoy
- They're finding it difficult to think or talk about much else

Enforced breaks from screens can have a dramatic effect and highlight issues of addiction or dependence

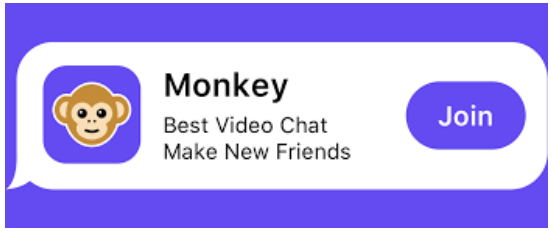
Social Media

- Mainstream social media is increasingly not very ‘Social’. It is almost exclusively used by children to consume professionally produced content.
- Some content encourages viewers to adopt certain values and can influences their aspirations and behaviours. Ultimately this will influence cultures.
- Focus is increasingly about comments and likes, and children can obsess about this as a method of validating their success and status.
- A lot of content can encourage unrealistic perceptions of reality and factors like body image. Children are often not good at identifying when filters are used.

Social Media

Ofcom's 2023 'Children's media lives', identified:

- Arguments between children and their peers played out publicly on social media
- Membership of large group chats is seen as a sign of status and popularity
- Young children are unable to identify fake accounts
- Accounts identifiable as children's, particularly girls, receive inappropriate explicit messages content
- Children sometime use less well-known apps to connect with strangers online. These platforms are often promoted by influencers



Social Media Age Restrictions

Under 13
(with parental consent)

GoBubble

PopJam

GROM SOCIAL

13 +

Facebook

Instagram

Tumbler

Twitter

Skype

iTunes

Pinterest

MyLOL

Wink

Snapchat

TikTok

reddit

ASKfm

16+

WhatsApp

Telegram

17+

18+

Meow Chat

Meet Me

Tinder

18
(13 with parental permission)

flickr

YouTube

Spotify

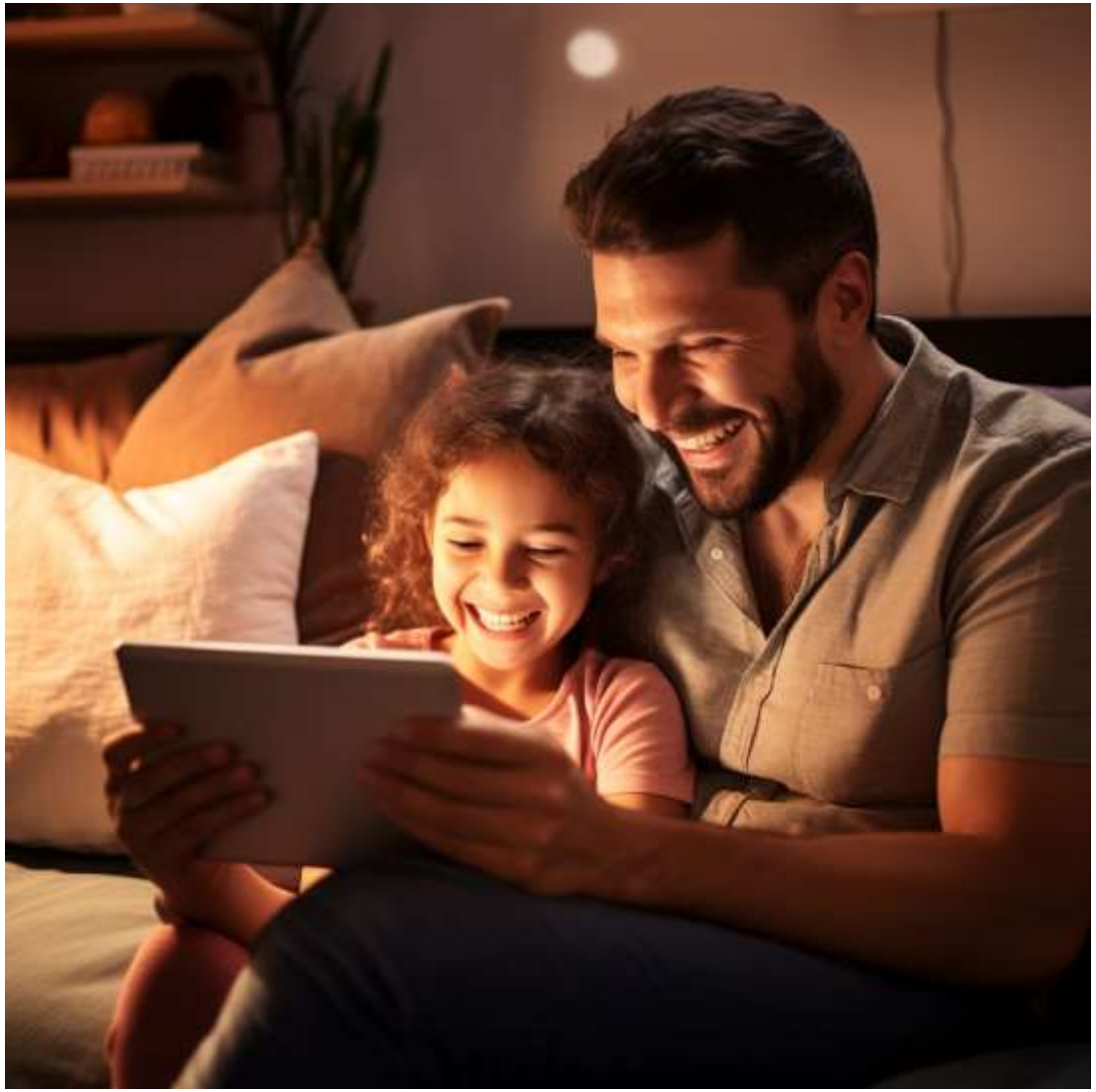
Learning

- Social media is increasingly being used for learning and being used like a search engine to answer questions
- Children generally believe what they see, read and hear on social media without considering its reliability or relevance.
- Children struggle to understand ranking of sponsored results or results provided by recommendation engines
- Most news is consumed through social media, rather than via news providers
- Recognisable logos and ‘blue ticks’ are perceived as signs of trustworthiness

Photographs and Videos

- Smart phones give the ability to take photos and videos of others, which is fun and exciting.
- Children may not understand why consent and privacy is important, even for everyday activities.
- Recordings and captures can persist on devices and online.
- Videos and photos can be shared, and subjects may not want this. This is especially true if relationships change over time.
- There are safeguarding issues with some children that their peers will not be aware of.

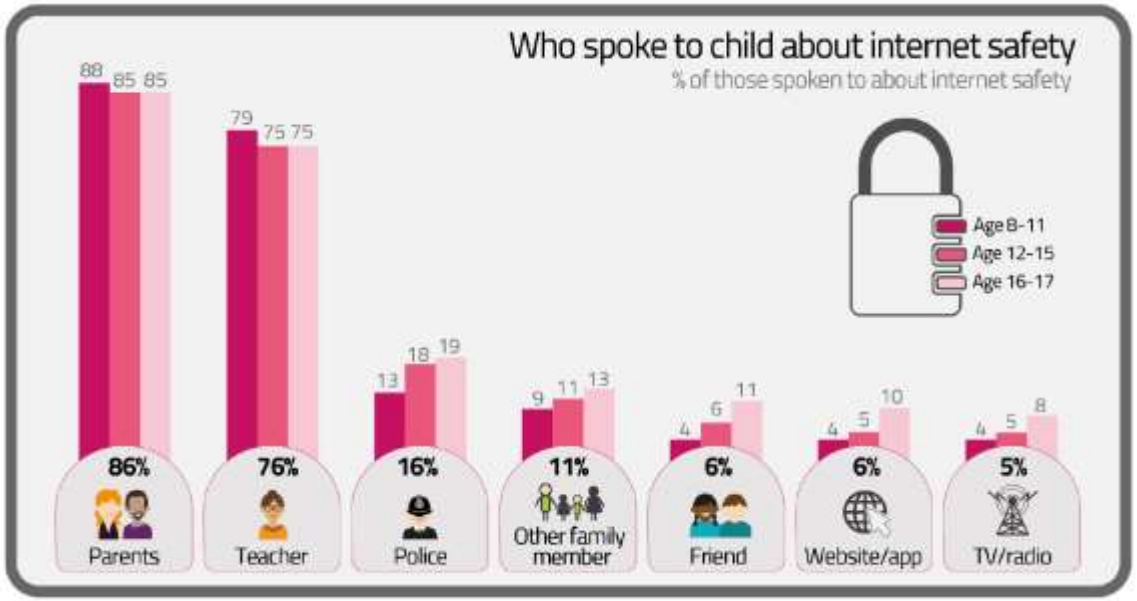
What can we do about it?



Conversation

Talk openly about online activities and online safety

- What are their needs?
- What do they want from you?
- What are your worries?
- What do you need from them?
- How they should respond to inappropriate behaviour or content when they encounter it



Protective Actions

- Action take 3 main forms:
  - Technical – Parental controls, time or content filters
  - Procedural – Rules, which can be backed up my monitoring
  - Physical – Taking away devices, or preventing access
- Layer multiple measures – DEFENCE IN DEPTH
- Appropriate balance will be individual to your own children and situation
  - Understand and prioritise your concerns
  - Use this to inform what measures you want to put in place
  - Over-restriction can lead children to conceal behaviour

Parental controls and monitoring

- Decide if monitoring or control is more valuable. Children's response to these may be different.
- Both can be useful but are not a one-stop solution
- Scope is often limited due to in-built privacy and security measures in devices
- Device and network level controls are more effective than third-party software
- Parental controls can be configured in some WiFi routers
- Many controls and monitoring can be circumvented. Instructions are easily found online if children are motivated

ICO’s statement on parental controls and monitoring*

Parental controls and monitoring impact on the child’s right to privacy as recognised by Article 16 of the United Nations Convention on Human Rights…

Children who are subject to persistent parental monitoring may have a diminished sense of their own private space which may affect the development of their sense of their own identity. This is particularly the case as the child matures and their expectation of privacy increases.

Make it clear to the child if parental controls are in place and if they are being tracked or monitored

* Abridged for presentation

Content Filtering

- Filtering can be applied at network or device level
- Different solutions can block types of content, or specific sites or services
- Some solutions can be technically complex to set up
- Some solutions can impact other users of those devices or networks
- Can be circumvented if children are technically savvy

Privacy and security settings

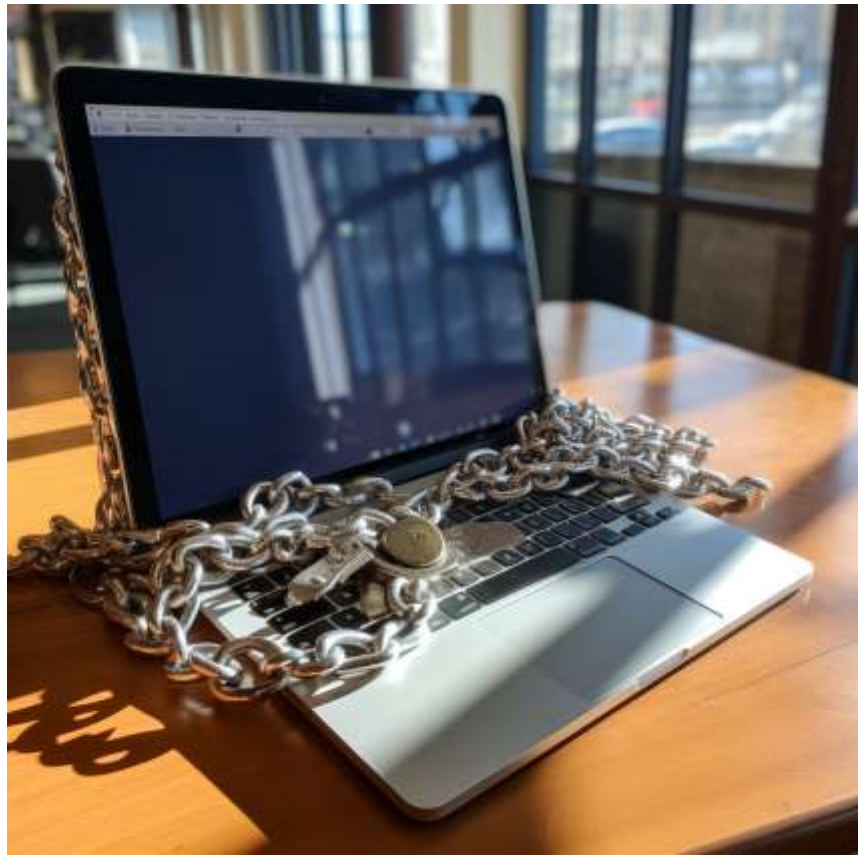
- Many apps and devices have privacy settings which need to be actively managed and regularly reviewed
- App updates can reset privacy settings
- Some settings are applied on the devices, and some are managed in the apps
- Many apps rely on access to private information for funding.
- Paid for versions of apps sometimes have better privacy
- Age related content and features can also be configured in some apps and games

Passwords and password managers

- Password are a fundamental security mechanism and children are not good at remembering passwords.
- Crazy website password strength rules make it **really hard** for anyone to use password without a password manager.
- If passwords can be guessed or become known, this can lead to cyberbullying, where bullies take over accounts or snoop on others.
- Many password managers offer ‘family’ subscriptions where parents can see and/or manage the passwords for their children’s accounts.
- Visibility of the site and services children are using, and how often.
- Additional security scanning, such as password compromise alerts.

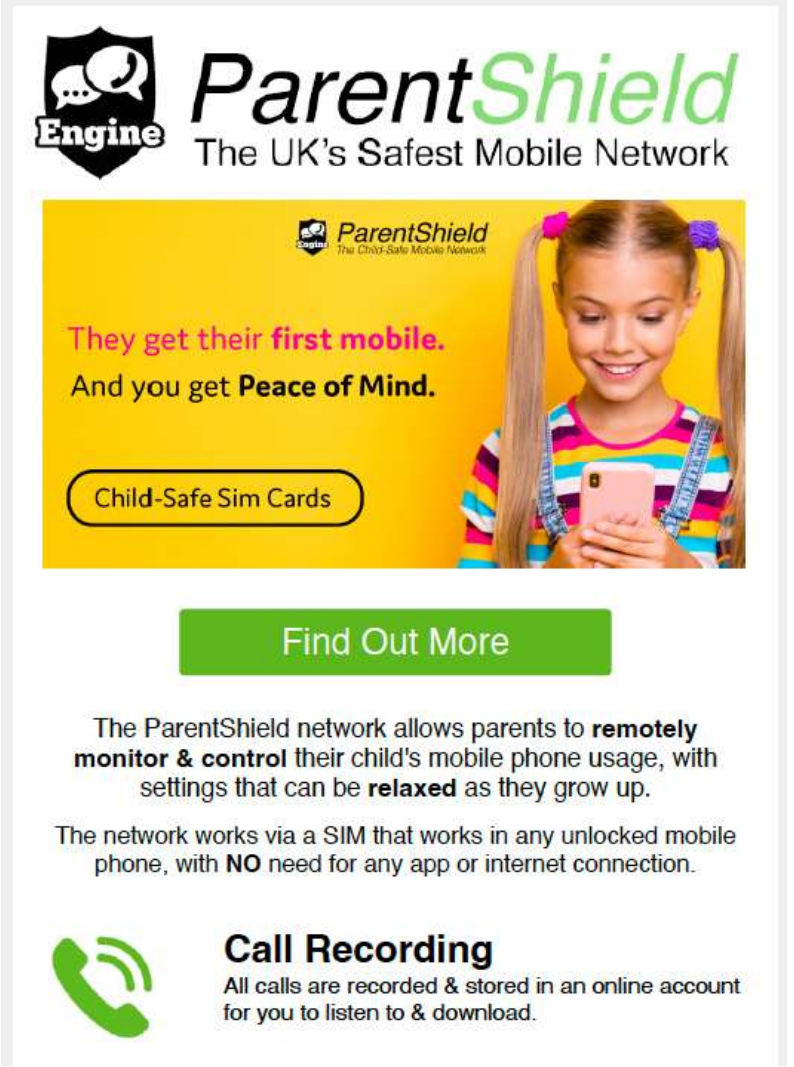
Accounts and permissions

- Many devices allow accounts to be created with limited access.
- Create children their own accounts on devices with limited permissions. For example, a non-administrator account on a windows PC.
- Security principle of Least Privilege
- Prevent children from installing software and changing configurations
- Limits potential for malware



Mobile phones

- There are many different options for mobile phones and contracts. Very few are focussed on children
- Mobile phones can offer a way around many parental controls and monitoring
- Child focussed sims such as ParentShield offer parental controls and monitoring at the network level
- In combination with device level parental controls this can provide a high level of monitoring and control
- As children grow and become increasingly responsible, control and monitoring features can be reduced
- Features include:
  - Time based network access rules with exceptions for home numbers
  - Text messages and calls are recorded and can be replayed by parents
  - Activity monitoring
  - Whitelist or Blacklist options for calls and messages
  - Spending restrictions



Rules

Rules must be designed to meet your priorities, but some examples are:

- Children must share device passwords or pins with parents
- Use of some services may require parental approval e.g. YouTube
- Installing any new apps requires parental approval
- Screen Time is only allowed between set times, or when certain criteria have been met
- Use of screens requires parental approval
- Only use devices in shared areas, not when alone in bedrooms

Be mindful that other parents may have rules and values that differ from your own.

Email

- An email address is often required to create online accounts and for multi-factor authentication
- Children can independently create email accounts out of view
- Creating an email account for your child gives you control. You can add this to your own devices for full visibility of their email activity
- Monitoring their email account will give insight into their online activity (and ensure they are not missing things)

Child friendly social media

A managed introduction to social media for young people

- PlayKids Talk (4+)
- GoBubble (4+)
- Grom Social (4+)
- Messenger Kids (6+)
- Spotlite – formerly Kudos (8+)