NEWS

FOLLOW THE FOOTPRINTS

Children's digital footprints – the body of information that exists on the internet as a result of online activity relating to them – are now vast. By the time they reach the age of 13, the average child will have had 1300 photos and videos of them posted to social media by their parents. And children between 11 and 16 will themselves post on social media on average 26 times a day – which means by the age of 18 they are likely to have posted 70,000 times (Office of the Children's Commissioner, 2018).

But it is not just social media. A new report from the Office of the Children's Commissioner for England – *Who knows what about me?* – explores how huge amounts of children's data are collected through the screens they watch, the websites and apps they access, through smart speakers, tracking watches, school databases, classroom apps, biometric data in schools, retail loyalty schemes, travel passes and medical records.

Even the youngest children are not exempt, thanks to a new wave of internet-connected interactive toys aimed at children as young as three. Last year, two million voice messages gathered by CloudPets – app-connected cuddly toys which allow children and their family members to share recorded messages via the internet – were found to be stored unprotected online.

DIGITISED FROM BIRTH

As the report points out, this is the first generation to be 'digitised' from birth, growing a vast digital footprint that has the potential to shape their lives now, and as they mature, in ways which neither they, nor the adults around them, can fully appreciate.

Not only can these bodies of data reveal personal information that could put them at risk of bullying or abuse, but the report warns that this generation will be at an increased risk of identity theft and fraud as they grow up. Their data profile could influence the adverts they are targeted with, and even whether they are offered a job, insurance or credit in the future.

Aside from this, there is the matter of a child's right to freedom and independence, and the question of how these children can understand their right to privacy, when they and others share personal information so readily.

As Anne Longfield, the children's commissioner for England, emphasises: 'We simply do not know what the consequences of all this information about our children will be. In the light of this uncertainty, should we be happy to continue forever collecting and sharing children's data?'

Work certainly needs to be done in policy and education, and action taken by companies producing these toys and apps.

The report makes a number of recommendations to that effect, including calling for clearer packaging on products that capture information about children, and new lessons in schools to help children understand how and why their data is collected.

A spokesman for the Information Commissioner's Office (ICO) says that its forthcoming age-appropriate design code for providers of websites, games and apps will be 'a key step in ensuring that providers of online services take their responsibilities to the children who use their services seriously, and design their products with children in mind'.

But what can be done on an individual level? What do practitioners need to know? And how can they best advise parents navigating this unfamiliar territory?

Today, the average child's digital footprint is broader than ever. What do community practitioners need to know when it comes to advising parents and helping to safeguard children?

'THE TRICKIEST OF TASKS'

From sharing birthday messages that show a child's date of birth, to 'first day at school' photos, which often reveal a child's location or identity through details such as school logos and street signs, the potential to unwittingly create risks is huge.

Anne says: 'Oversharing by parents can be a problem on lots of levels. Too often we find the child hasn't even been asked, or if they have expressed a negative feeling about it, been ignored.

'Nobody should be saying parents mustn't post anything – that's unrealistic and frankly silly, but again the dialogue with children about this is crucial. Practitioners have that trickiest of tasks to make judgement calls about this, and the best thing is to start with some kind of dialogue with the parent.'

'CPs ARE IN A KEY POSITION TO EDUCATE AROUND SAFE USE OF THE INTERNET, DATA PROTECTION AND EXPLOITATION'

Anne accepts that tackling parents' personal choices is harder than clear-cut safeguarding issues. 'Often just outlining who owns an image, how many people can see it, what it might say about the child that possibly hasn't been considered and, it won't surprise you that I say this, what the child's view about it is, will often at least get parents thinking a bit more about the issue.'

She continues: 'Advise families to think about who and for what reason they are giving their data

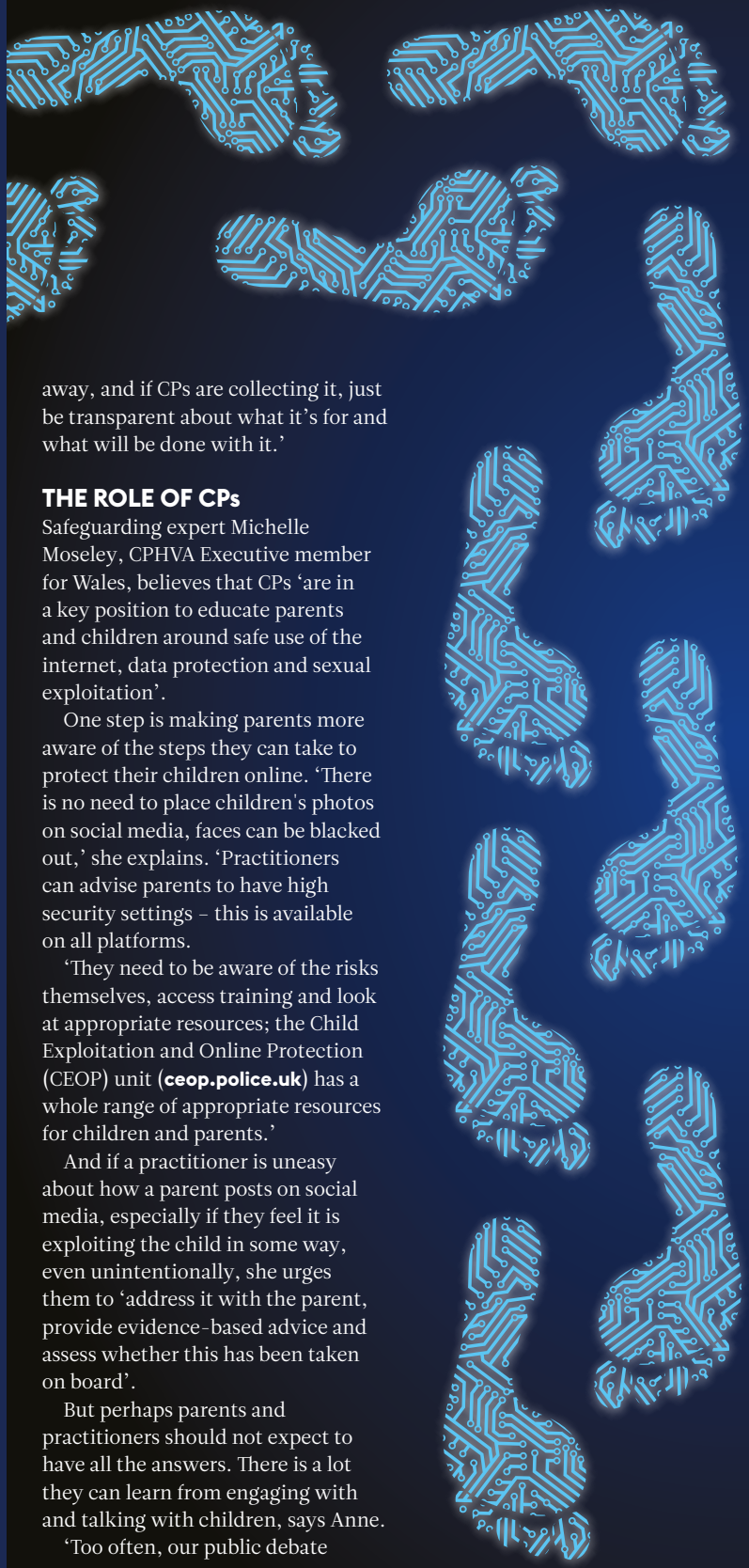
TOP 10 TIPS FOR STAYING SAFE ONLINE

FOR CHILDREN

1. Stop and think when you're about to share some personal information.
2. Read the Digital 5 a day guide if you spend lots of time online and on social media at **bit.ly/CCE_5_a_day**
3. Look through terms and conditions to see what data is collected when you use websites and gadgets at **bit.ly/CCE_TandCs**
4. Mute smart speakers when you don't want them to listen to you.
5. Talk to an adult you trust if you are worried about someone else knowing something about you.

FOR PARENTS/CARERS

6. Don't post photos and videos which reveal personal information about your children.
7. Change the default passwords on all the gadgets your children use.
8. Make sure the gadgets you buy your children are genuine. Counterfeit versions can be even less secure.
9. Watch out for security updates and install them as soon as you are prompted.
10. Talk to organisations that hold information on your child about what information they collect and why.



away, and if CPs are collecting it, just be transparent about what it's for and what will be done with it.'

THE ROLE OF CPs

Safeguarding expert Michelle Moseley, CPHVA Executive member for Wales, believes that CPs 'are in a key position to educate parents and children around safe use of the internet, data protection and sexual exploitation'.

One step is making parents more aware of the steps they can take to protect their children online. 'There is no need to place children's photos on social media, faces can be blacked out,' she explains. 'Practitioners can advise parents to have high security settings – this is available on all platforms.

'They need to be aware of the risks themselves, access training and look at appropriate resources; the Child Exploitation and Online Protection (CEOP) unit (**ceop.police.uk**) has a whole range of appropriate resources for children and parents.'

And if a practitioner is uneasy about how a parent posts on social media, especially if they feel it is exploiting the child in some way, even unintentionally, she urges them to 'address it with the parent, provide evidence-based advice and assess whether this has been taken on board'.

But perhaps parents and practitioners should not expect to have all the answers. There is a lot they can learn from engaging with and talking with children, says Anne.

'Too often, our public debate around children is adults talking to other adults about what another set of adults should do for children,' she says. 'That should be the end of the process, with the start cutting out all those adults and just talking with children.

'We have found giving advice is fine, but providing frameworks for children and adults to have their own discussions about something is actually more effective.'

And while she finds that children in the UK are 'actually pretty savvy about safety issues and often well advised on what to do and not do to stay safe', there is a need to address other issues which 'don't really come under the banner of safety'.

EDUCATING CHILDREN – AND OURSELVES

'We need them to learn that things you wouldn't do in real life are not appropriate in a digital sense, that it doesn't make them lesser people if their photos don't get hundreds of likes, that sending people vicious messages direct to maybe their bedroom late at night is not behaviour that can or should be tolerated – asking themselves always "Do I want to post this?" and "Who am I really talking to?"'

Anne doesn't want to see children online shut up in 'some digital backyard'. 'But we need them to be armed with the tools to explore both safely, and confident in the knowledge that they know what's what and how to handle it without upsetting their overall wellbeing.'

As the report says, educating children 'early and comprehensively about the many ways in which their data might be used is an important way to foster digital resilience and to help rebalance the power between children and those that gather or use their personal information'.

But, with these digital natives far more at home in this space than the adults around them, perhaps we must first take steps to better educate ourselves.

FURTHER GUIDANCE

- Parentzone offers a free online safety guide to digital family life at **parentzone.org.uk**
- ThinkUKnow raises awareness of online child abuse and exploitation at **thinkuknow.co.uk**
- Childline offers children advice on taking care of their digital footprint at **bit.ly/childline_digital_footprint**

For references, visit **bit.ly/CP_news_big_story**