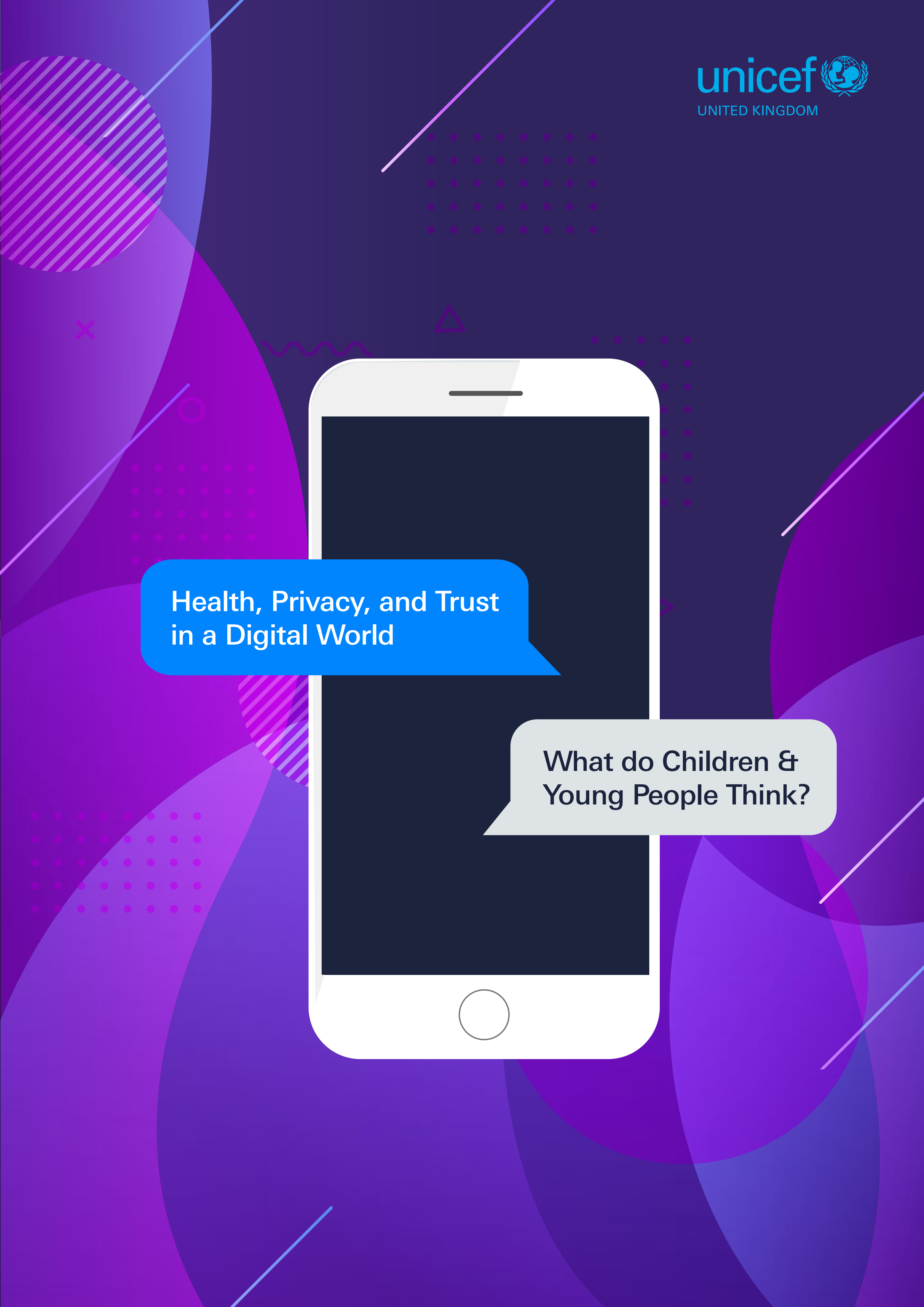
unicef
UNITED KINGDOM



Health, Privacy, and Trust in a Digital World

What do Children & Young People Think?

Introduction

Digital technology has already changed our world – and as more and more children go online, it is also impacting their experience of childhood. More than 9 out of 10 children in the UK aged 5–15 go online, and this increases with age, ranging from 52% of 3–4 year olds to 99% of 12–15 year olds.[1] Children in the UK are also among the youngest in Europe to go online – at an average age of 8.[2]

Unicef UK advocates for the full realisation of children's rights in a digital world, including the right to privacy. Children should be empowered to take advantage of the opportunities of being connected – to share, to learn, to play, and to participate, while they must also be protected from the risks that await them online. Businesses have a critical role to play in making this a reality. As recognised in the UN Guiding Principles on Business and Human Rights, companies, including those in the ICT sector, have a responsibility to respect human rights. The Children's Rights and Business Principles, published by UNICEF, the UN Global Compact, and Save the Children, further clarify that businesses have a specific responsibility to respect children's rights and should, among other things, ensure that their products and services are safe for children.

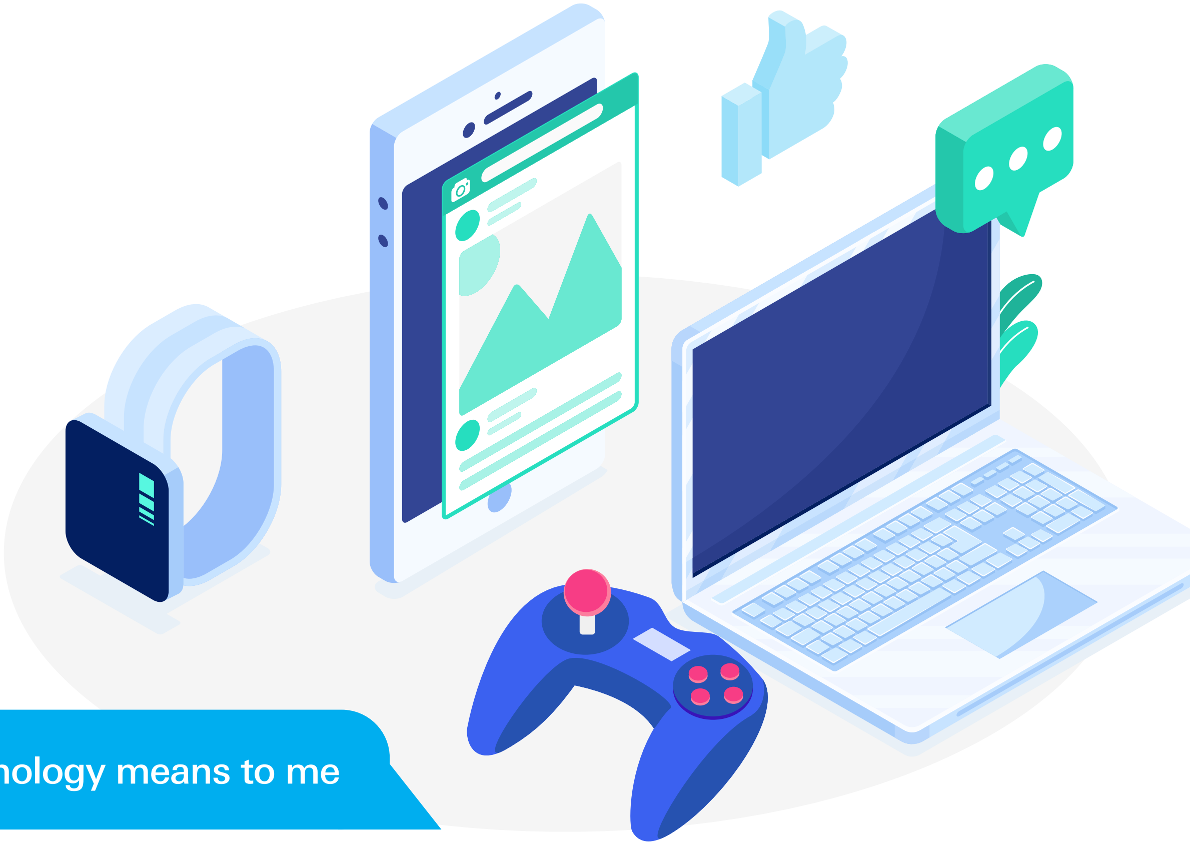
Moreover, children have a right to have their views heard. With digital technologies playing such a central role in children's lives, it is also more important than ever that these views and experiences are heard and acted upon by government, businesses, and civil society organisations to ensure that children's rights are protected, respected, and supported online.

To ensure that children's voice are reflected in this work, Unicef UK spoke to 19 children and young people (aged 11 to 19) at participatory workshops in two cities in Northern Ireland and Northern England between July and August of 2019.[3] These were held as part of a global consultation developed and coordinated by Western Sydney University, 5Rights Foundation and the London School of Economics and Political Science (LSE) to inform the drafting of a new General Comment by the UN Committee on the Rights of the Child on 'Children's Rights and the Digital Environment'. Unicef UK wishes to acknowledge and thank the children who participated in these focus groups for their insights and enthusiasm.

[1] Children and parents: Media use and attitudes report 2018, Ofcom

[2] EU Kids Online, LSE: http://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/participant-countries/uk

[3] 6 male participants and 13 female participants contributed across the two cities.



What technology means to me

As one participant put it: **'I can't imagine my life without the internet'**. Some recalled how young they were when they first got a phone; others how checking their social media accounts is the first thing that they do after waking up. The benefits of access to technology were deeply appreciated by all, including the power of instant access to information whereas **'before, you'd have taken hours to go to a library'**. This reliance could be seen in the amount of time that participants spend online each day – one was even alarmed to discover (during the workshop itself) how many hours a week they spend on the internet.

The children and young people grappled with the difference between 'wants' and 'rights' when it came to access to technology. Although the group members had a wide range of previous exposure to the concept of 'rights', almost all were able to correctly identify rights from wants. Recognising that it is not as essential as health or nutritious food, one participant explained that **'I can and can't live without social media.'** The difficulty of functioning fully without technology led four participants to designate **'using a laptop computer'** as a human right, one explaining that this is essential **'for educational reasons'**. Three participants counted having a mobile phone as a human right as well as a want, with one qualifying that this **'can be a future right'** as technology becomes an increasingly essential part of daily life.

When considering the different articles of the UN Convention on the Rights of the Child, the group recognised how the same rights can be both positively and negatively impacted by digital technology, depending on the situation. To name one example, children's right to be protected from the illegal use of drugs (Article 33) can be positively impacted, as children can learn about the dangers of drugs online, but also negatively impacted because of **'dangerous drug videos and photos online that can influence younger people'.**

Is technology **good** for us?

Both groups spent time thinking about how digital technology can be used in 'healthy' and 'unhealthy' ways. Six major themes emerged when talking about 'healthy' uses, and four main categories of 'unhealthy' uses. The topics below are listed in order of how often they were raised by all participants as a group:

Top **'unhealthy'** uses of Digital Technology

Spending too much time online

Summary: It is easy to spend too much time online, which means you don't go outside or talk to friends enough. People might also become less sociable and have weaker social skills.

'Spending too much time online and then half your day is gone. You never get a break'

'Realise it's 3 pm and I've f***** up again and missed morning'

'Phones may replace friends'

Mental health and self-esteem impacts

Summary: Being online can hurt mental health and make you feel depressed and anxious or lower your self-confidence by seeing unrealistic photos. It can also make you feel pressured to conform, to maintain 'streaks' (unbroken back and forth connection with someone on a messaging platform) and to fit in or act like famous celebrities. It also hurts when people share personal information online.

'Social media impacts body image'

'Confidentiality broken (…) Hurts both physically and mentally. Impacts confidence and self-esteem'

'Never get a break'

Physical health problems

Summary: Spending too much time online can hurt your health by disrupting sleep, replacing physical activity, or impacting eyesight. Information that is harmful to health, like anti-vax messages, can also spread rapidly online. Some were also worried about potential injury from phones and chargers overheating.

'People spend more time on their phone than doing physical activities'

'Missing out on vitamin D staying indoors'

'Scraps, fighting, bullying. If something happens, you know it right away'

Cyberbullying and conflict

Summary: Cyberbullying and fights can happen online.

Online violence and crime

Summary: There can also be predators, abuse, harassment, grooming, and inappropriate content. It's also possible to buy drugs like weed online.

'Grooming by older men'

'Get what you want online – drugs'

Top **'healthy'** uses of Digital Technology

Accessing new information

Summary: Instant, easy access to new information makes it possible to teach yourself new things like foreign languages or news about the world. Websites like BBC Bitesize, YouTube, and others help with homework and revision.

'Greater knowledge of world affairs due to widespread news accounts'

'So much potential to educate yourself like never before'

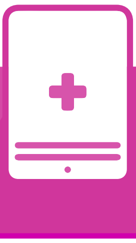
Staying in touch with others and building relationships

Summary: Technology makes it possible to connect with loved ones like family members no matter how far away they are. It makes communication easier and helps to build new relationships as well as distracting you and helping you to relax.

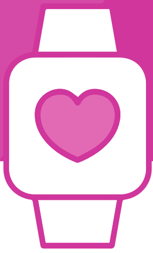
'You can find family members online'

Preventing and treating diseases

Summary: Advances in medical technology can keep people alive and help to diagnose illnesses. Apps and other technologies like Fitbit can help to keep you healthy and active.



‘Improve healthcare (AI/3D printing) and sending scans to the other side of the world’



Improving safety for children

Summary: Access to technology helps to stay in touch with parents and friends to make sure you are safe. You can also report bullying or other problems online. Tools like Google Maps can also help to avoid getting lost, which also gives you more independence.

‘Communication with parents and friends so they know where you are and you’re safe’

Having fun!

Summary: The internet can help to distract you and get your mind off other things. You can listen to music and enjoy reading friends’ posts.

‘It’s good craic reading everyone’s posts’

‘You can take your mind off things’

My data, **my rights**

Fifteen of the participants were asked to respond to four statements about their privacy online. As the results and quote below illustrate, children are not wholly willing to forego their privacy in order to access services. Indeed, many care deeply about their data rights.

Statement 1:

I don't care if social media platforms own my images when I share them with my friends. Who would want to use my images anyway?

All respondents **disagreed**

'No because I feel as though my pictures should only be kept by me and not for profitable gain by others'

'Images are really personal and I hate the [use of] facial recognition'

'Digital rights are human rights'

Statement 2:

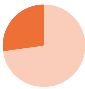
Social media platforms let me use them for free, so I'm not really worried about what they do with my data. It's a fair trade.

53%

of respondents **disagreed**

'Companies are using your data to make billions of pounds by selling it to companies that put your privacy and safety at risk. Are you still sure this is fair?'

27%

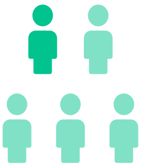


of respondents argued that **they should not be forced to make the trade at all.**

'Digital rights are human rights and it shouldn't be a trade'

'You should be able to trust a company with your data even if it is a fair trade'

20%



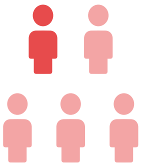
of respondents **agreed**

'If the social media platforms don't sell data, then they wouldn't be able to function.'

Statement 3:

I’m really worried about hackers who can break into data storage systems and use my data.

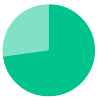
20%



of respondents **disagreed**

‘There will always be a risk of hacking, the same as robbery’

73%



of respondents **agreed**

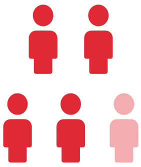
‘Your data is never safe.’

One participant explained how the risk of hacking worries them when it comes to sharing data with institutions that are otherwise trustworthy: **‘I trust the NHS with my data but don’t trust their ability to protect themselves from cyberattacks.’**

Statement 4:

I have all my privacy and security setting on, so I’m not really worried about my data.

79%

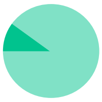


of respondents **disagreed**

‘There are many things we simply agree to that are even on the highest privacy settings.’

‘There are so many ways your data can be collected so it’s impossible for privacy settings to cover everything.’

14%



of respondents **agreed**

‘If security settings are on then you don’t need to be worried.’

One participant made the point that it is not possible to judge whether it is necessary to worry, because the facts are not clearly communicated to users: **‘We’re not educated enough to know if this is enough.’**

What we want to know about **our data**

Both groups expressed a strong appetite to learn more about how their data is used and how to manage their privacy online. Participants had many questions, some of which are displayed below. A large number wanted to know more about how their data is monetised by companies, and who can access it.

‘Who uses it? What is it used for? Can I keep it safe? How long do you keep it? Can I get it back?’

‘EVERYTHING. Your data is your property. Fundamental right to know how it’s being used. How easy would it be to misuse my data and is it being monetised?’

‘I would like to know how they got the information.’

Several participants expressed a concern about how their data can be used to manipulate their thoughts or actions, with several making reference to a recent documentary, The Great Hack, and the Cambridge Analytica scandal. They wanted to know more about these practices:

‘What do they use (my data) for? Do they try to influence my thoughts and feelings?’

‘Is my data used/or will it be used to manipulate me?’

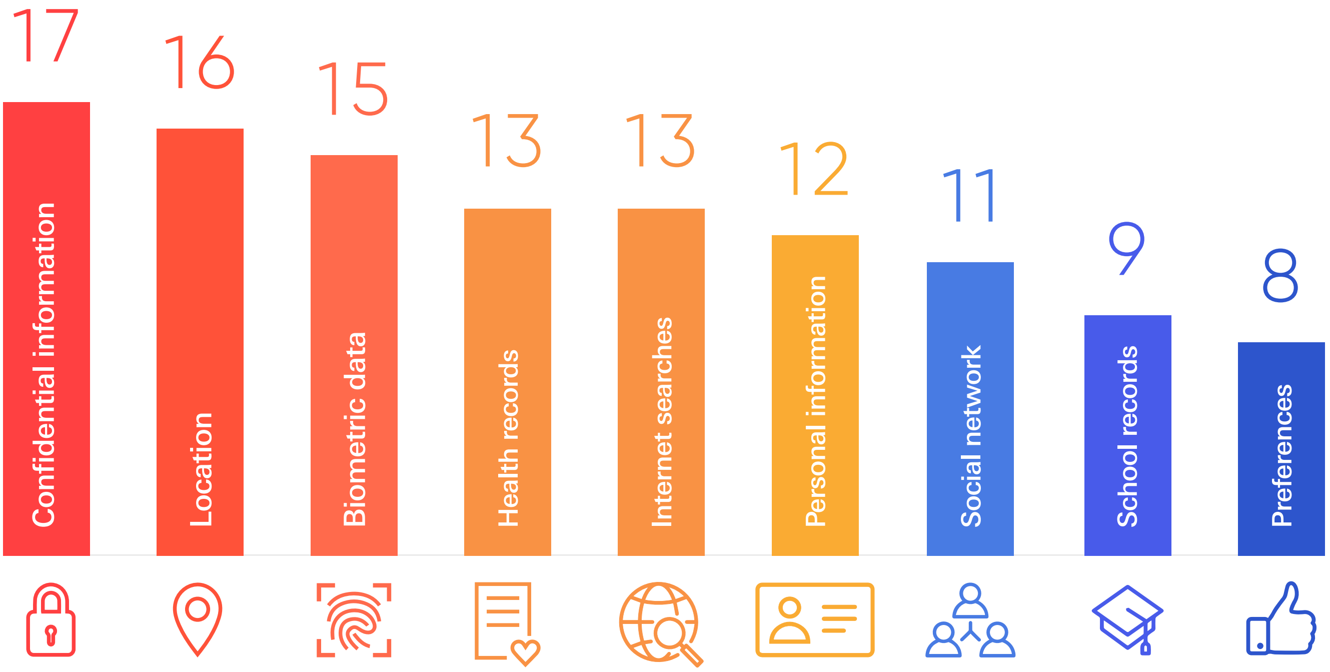
‘That amount of data can be used in many bad ways that could (…) manipulate people into doing things that they wouldn’t usually do.’

Given this high level of interest and concern about personal data, both groups discussed which forms of data they would be willing to share and with whom.

Who **needs** to know?

Personal data can take many different forms, from information about where you are to your previous internet searches or records about doctor's visits. Participants felt differently about each of these types of information and were less willing to share some than others.

Number of participants who said they would prefer to keep this information to themselves

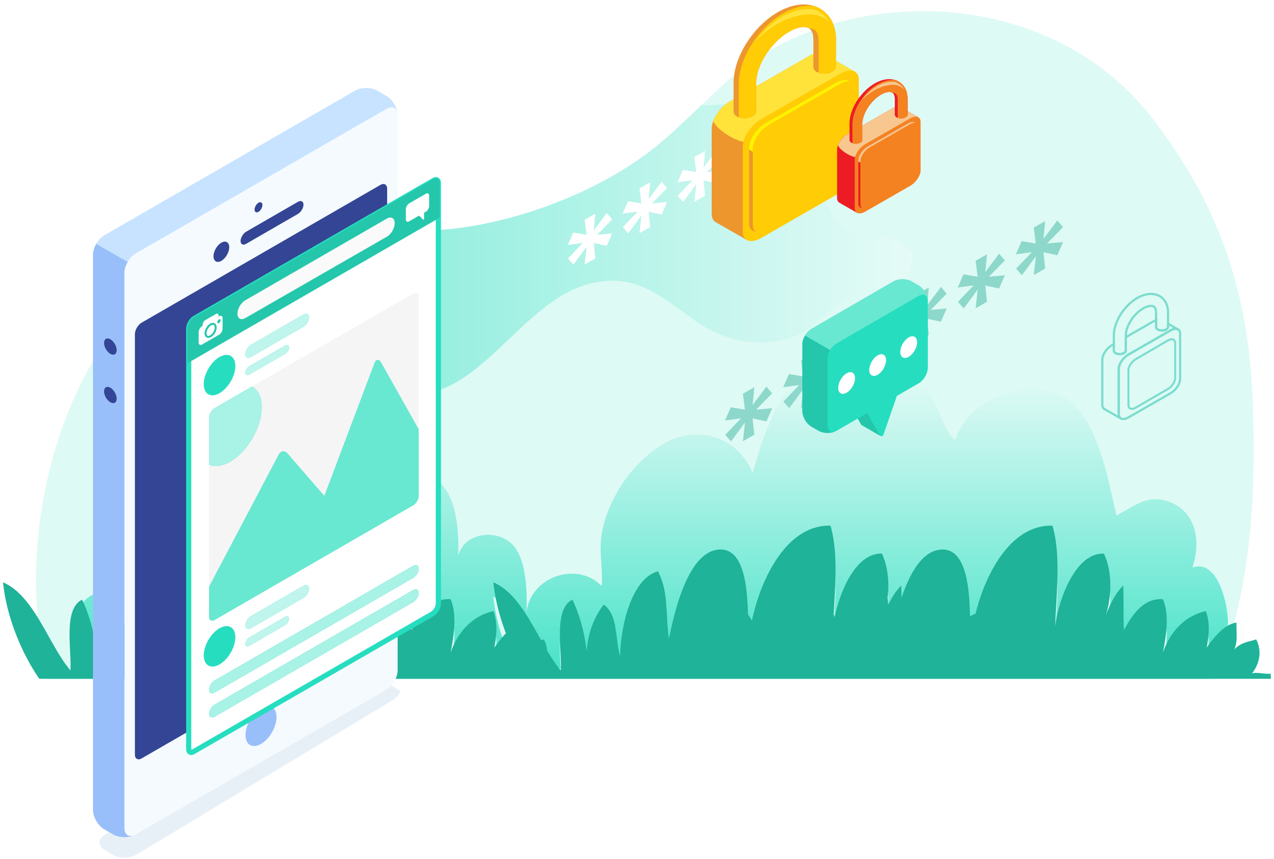


Although a large number of participants signalled that they would prefer to keep their personal information private, most also agreed that they would be willing to share this with their school, doctor, or future employer (along with health records and school records).

In general, the group was quite unwilling to share information with online contacts. While 8 said that they would share their preferences and 5 their social network, the other categories of information received a much lower response (with a maximum of 2 participants saying they would be willing to share these with online contacts).

Only 1 person said they would be willing to share confidential information with companies. Likewise, only 2 said they would share biometric data and health records with them. Overall, participants were most willing to share their preferences (8 respondents) and internet searches (4 respondents) with companies.

This clash between the desire not to share information and practical situations where this is made difficult also came up in conversation. One participant explained that: **'I only got Facebook a week ago. [A youth group] needed me to join, so I had to get an account. I really didn't want to do it but there was no choice. That's just how it's done.**' This was shared by several others, who felt that they generally have little control over the sharing of their data partly because this has become **'normalised'**.



Confidentiality, safety, and social media in small communities

Some participants expressed a strong desire to be able to keep as much information as possible to themselves. In general, they did not appreciate details about their lives being shared with others, like when adults who work with them sometimes talk about their private lives in front of other young people.

In the context of a small community where people have a lot of access to information about each other's lives, the issue of how social media is used to spread information is a real concern for young people. This is partly because of safety worries arising from sensitive information like location being broadcast, but also because of the distress associated with learning troubling personal news online. For example, news that friends have gone missing can be found on social media as posts are made and shared rapidly.

'I found out [a family member] died on Facebook. I didn't know.'

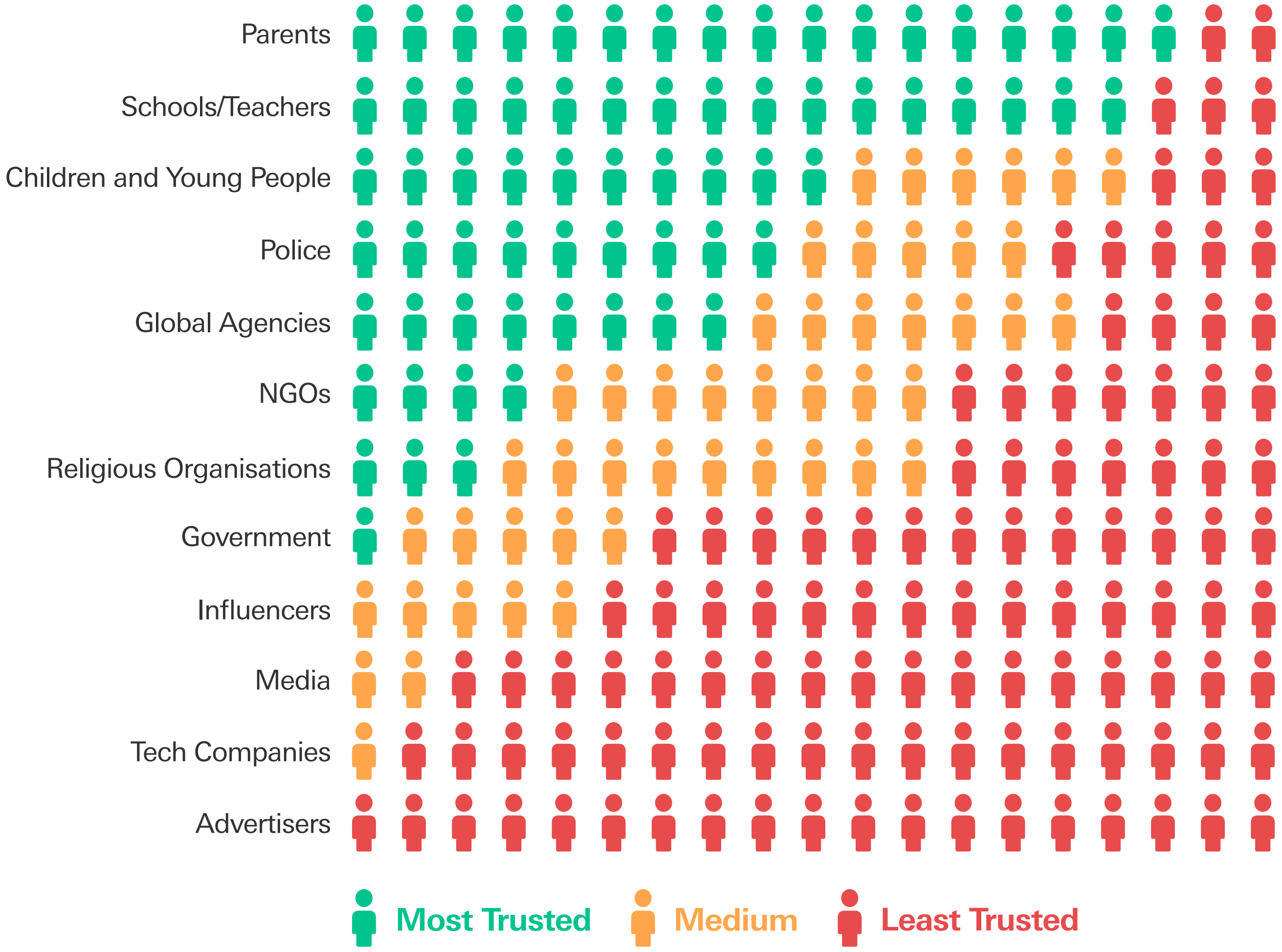
'When you add a photo on Facebook then people know where you are and they can come beat you up!'

However, the desire not to share information contrasted strongly with the level of understanding regarding privacy settings on social media accounts. One participant discovered during the session that several pieces of personal information were in fact public (including phone number, parents) and would be accessible to a very large number of contacts. This illustrates the importance of high default privacy settings for children.

Who can we **trust**?

We asked all 19 participants which groups and organisations they trust the most to help them have good experiences with technology. Parents and schools and teachers were overwhelmingly the most trusted, while advertisers, the media, and tech companies were the least trusted by many, as one participant explained:**'I don't trust media, advertisers, tech companies and influencers at all as they just expose our data, share it with other companies and unfortunately monetise from it.'**

Most trusted to least trusted



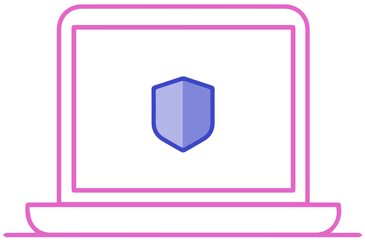
Some members of the group expressed a very low level of trust towards others in general. One participant put this quite simply: **'I don't trust anyone'**. As in the figure above, for several this extended to mistrust of authorities. We learned that several were not aware that their phones can track their location, but there were suspicions that phones were bugged by the police, which gave rise to more general reflections about poor and mistrustful relationships with the police: **'My phone is tracked by cops. Cops have my phone bugged'**. This highlights how young people's relationship with technology can differ widely based on their contexts, with some worrying that their devices can be used against them.

Fifteen of the participants were also asked to consider the roles of each of the groups above in more detail. They reflected on which had the most responsibility to complete each of 9 tasks including to 'protect my safety online', as well as which were most trusted. As the results below illustrate, those groups that the young people perceived as having the most responsibility were not always seen as the most trustworthy. Out of the 15 respondents, the number who voted for each group is also displayed below in brackets.

Protecting my safety online

Most responsible:
Government (13)

Most trusted:
Parents (10)



Developing online safety products for me

Most responsible:
Government (14)
Tech Companies (12)

Most trusted:
Government (4)
Tech Companies (4)
NGOs (4)

Protecting me from companies who might want to use my data

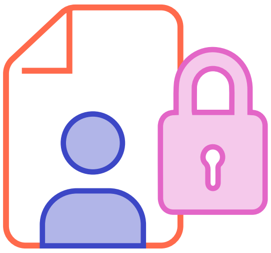
Most responsible:
Government (15); Police (8)
Tech Companies (7)
Global Agencies (7)

Most trusted:
Parents (8); Police (8)
Schools and Teachers (7)

Keeping my data private

Most responsible:
Government (13)
Tech Companies (11)

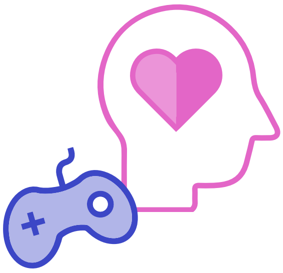
Most trusted:
Parents (11)
Schools and Teachers (9)



Developing games that are good for my mental health

Most responsible:
Tech Companies (12)
Global Agencies (9)

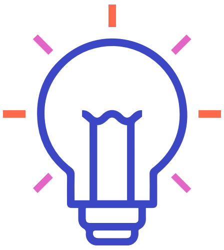
Most trusted:
Children and Young People (7)
NGOs (6); Schools and Teachers (6)



Teaching me creative ways to use digital technology

Most responsible:
Schools and Teachers (14)
Influencers (7)

Most trusted:
Schools and Teachers (11)
Parents (9)



Helping me learn good digital media habits

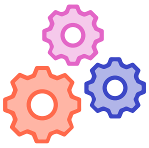
Most responsible:
Schools and Teachers (14)
Parents (9)

Most trusted:
Parents (12)
Schools and Teachers (11)

Helping me learn how to use new technologies

Most responsible:
Schools and Teachers (14)
Parents (8)

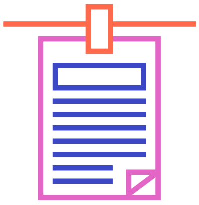
Most trusted:
Schools and Teachers (11)
Parents (7)



Protecting me from fake news

Most responsible:
Media (12)
Government (11)

Most trusted:
Schools and Teachers (10)
Parents (7)



The problem of fake news also appeared in conversation, with one participant complaining that **'Google tells you lies. Fake news.'**

While it was felt that tech companies have a number of responsibilities, including to keep data private and develop games that are good for mental health, they were only among the most trusted when it comes to developing online safety products. This suggests that tech companies can do more to earn the trust of young people by taking more steps to fulfil their responsibilities in the eyes of children.

What **changes** do we want to see?

Both groups considered what changes they would like to see in terms of how their online environments are designed and managed.

One participant was keen to see **'better protections to stop people contacting you'**. Another wanted to see changes in how companies collect and process data: **'it just creeps me out.'** More generally, we also asked what they think adults need to understand in order to make the digital world a happier, safer, more rights-respecting space. They told us that it's important that they know when young people are being bullied, that there should be **'no trackers and no cops'** and that listening to children and young people is key.

'they need to trust us and listen'

The group also set out the changes they would like to see when it comes to the management of their personal data and privacy online. Four major asks emerged:

Give us a choice

The option to opt out of sharing personal data should be easily accessible, and services should always ask for consent before accessing personal information.

'Easier access without giving away information – choice.'

'To be able to decide when and what our data is being used for.'

'Have more choice about whether to share your data, e.g. when accessing websites.'

Be more transparent

People should be able to find out exactly where their data is going, how it is being used, and why.

'Make it more open and accessible to know what you are sharing and who you are sharing it with.'

'I want to see a digital map of exactly where all my data is.'

Protect my data

Reassure people that their information is secure and protect it from cybercrime.

'Block ads or scams to access my private information.'

Educate people

Make sure to educate people so that they can understand what they are being asked to consent to.

'NEED MORE EDUCATION – people need to know what they're agreeing to.'

'Explain to people what cookies really are'

One participant clearly called for **'more legislation especially for under 18s'**, while another explained that they worry about what companies will do with their digital profiles in the future, which further emphasises the urgency of this issue.

Conclusion

The workshop outputs highlight the complexities and diversity of the participants' experiences of the digital environment. Throughout group discussions about the positive and negative impacts of the digital technology on the lives of children and young people, there was a clear message about the lack of accessible information and guidance on navigating the digital environment; and a general mistrust in media, technology companies and governments in ensuring that children and young people have positive experiences with technology. Many participants expressed a keen interest in learning more about online safety and how to understand and control how their data is being used.

Participants overwhelmingly expressed an interest in being consulted on this topic and having the opportunity to discuss and share their experiences and views of digital technology. It was apparent throughout the workshops that, as digital technology has an increasing impact on childhood experiences, there is a clear need for accessible tools and information to support these experiences to be safe, positive and healthy.

Supplementary Note on Participation Process and Next Steps

In carrying out this work, we committed to including children and young people from diverse backgrounds. We made sure that there was support for the sessions with local workers who had strong and trusting relationships with the groups. For us as external facilitators, the local support both for the young people's participation and for providing the local context was invaluable.

The Shared Space Agreement was an opportunity to reinforce informed consent among the group and to establish the respect and confidentiality arrangements needed for the workshop to continue. Young people were reassured by the workshop leads about the anonymity of their participation and that no photos would be taken of them, just of their work. Skilled and trusted youth workers were present throughout the session so that they could provide ongoing support for the young people if the workshop were to raise anything difficult for them and in order to take appropriate and proportionate safeguarding action if needed.

The session had been developed and adapted to cover the topics of trust, privacy, and health, along with mandatory exercises on child rights. We adapted the sessions as we went to accommodate and support the young people to take part in as much of the workshops as possible, in a way that suited them.

Overall, there was a strong desire among the groups to be able to keep as much information as possible to themselves online. This was in quite stark contrast to how their information was currently being shared online and their level of understanding regarding online privacy and how to keep data safe and confidential. In response to this, we provided materials and resources for the groups to engage with beyond the workshop on how to change privacy settings, how to generally protect privacy and how to stay safe online.

Participants were told about the opportunity to take part in further Unicef UK child rights bespoke training (an introduction to the UN Convention on the Rights of the Child adapted for children and young people) to strengthen their understanding of children's rights and the duties of those obliged to uphold and protect those rights.

Please contact:
UNICEF UK
1 Westfield Ave, London E20 1HZ
+ 44 (0) 20 7490 2388
Email: crb@unicef.org.uk