

Growing up in the online world: a national consultation from the Department for Science, Innovation and Technology (UK Government)

Response from the Scottish Council for Voluntary Organisations

The Scottish Council for Voluntary Organisations (SCVO) appreciates the opportunity to respond to the UK government's consultation '[Growing up in the online world](#)'.

SCVO is the national body in representing the voluntary sector (charities, social enterprises, and voluntary groups, aka third sector) in Scotland, with a membership of 3,000+ organisations. Our mission is to champion the sector's social and economic contributions, provide essential services and debate big issues. The sector in all its diversity is a powerful force for positive change across Scotland and a significant part of our economy, with over 46,500 voluntary organisations and over 800,000 volunteers. For further information please refer to SCVO's State of the Sector 2025.

This consultation touches on issues that are central to how we promote and support digital inclusion. SCVO has been leading the delivery of digital inclusion across Scotland for 15 years and continues to do so through a range of different programmes.

In preparation of our response we have engaged with organisations working with children and young people, with a particular focus on smaller organisations that may otherwise struggle to resource the time to respond to this consultation. Our response is therefore shaped by the views of childcare practitioners, youth parliament members, charity board members, digital safety experts, and third-sector organisations.

Our response has focused on 5 areas that are most relevant to our work on digital inclusion.

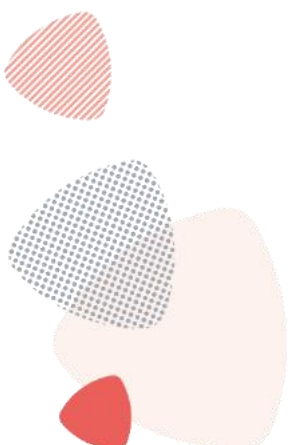


Organisations and Voices Represented

The following organisations and individuals contributed evidence to this consultation. Their thoughts are cited throughout this report, and they are referred to collectively as 'stakeholders':

- Seamab
- Kids n Clicks
- Y Sort It
- Scouts Scotland
- Member of the Scottish Youth Parliament (MSYP)
- Cake or Dice
- Strange Town
- Sewing Together All Nations
- National organisation working on behalf of children and young people

The consensus amongst stakeholders is that outright age-based bans are a 'false promise'. The evidence points instead towards Safety by Design, mandatory corporate accountability, sustained third-sector funding, and a public health approach to online wellbeing that treats digital harm on a par with smoking or road safety, alongside adult role modelling.





Chapter 1: Understanding how children use technology

- What are the benefits of social media use, and being online, for children?
- What are the harms or risks of social media use, and being online, for children?

Stakeholders acknowledge that while online connectivity is a vital tool for modern life, it remains an adult-designed space that children are navigating largely without adequate safeguards.

The internet is now woven into every aspect of childhood from homework and social connection to creative expression and career awareness. Young people's digital lives do not pause at the school gate, and any policy response must grapple with this inescapable reality.

The Benefits

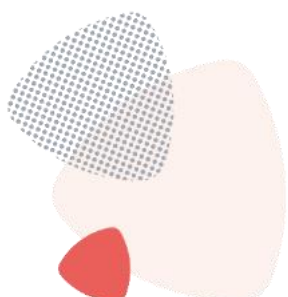
There is broad agreement that the primary benefit of social media for children and young people is connection and community. For young people who may feel isolated or marginalised in their offline lives including those who are neurodivergent, LGBTQ+, or living in rural areas, online spaces can provide vital peer support, identity affirmation, and a sense of belonging that is not available to them locally.

Stakeholders also identified significant educational and creative benefits. Young people use platforms to develop skills in content creation, digital entrepreneurship, and personal branding that have genuine career value. For some, the internet represents an equalising tool offering access to resources, communities, and opportunities that geography or socioeconomic status might otherwise deny them.

"I really see children that have a strong identity through it. They've got a sense of self... you can, through the creation of an avatar or creating achievement points, build something that feels genuinely meaningful to them." Seamab

The Risks

Opinion is significantly divided on whether the harms of social media ultimately outweigh the benefits. Several stakeholders argue that the systemic risks including addictive algorithms, exposure to harmful sexual or violent content, sleep deprivation caused by late-night device use, and the commodification of



children's attention are so deeply embedded in platform design that no amount of individual education or parental vigilance can fully mitigate them.

Others are more cautious about characterising the internet as inherently dangerous, arguing that with the right skills and frameworks, young people can engage with these platforms purposefully using them for achievement, business, and self-expression rather than passive consumption.

A further dimension of risk identified in our engagement is the impact on physical health. Screen time and sleep deprivation are increasingly recognised as interconnected concerns, with young people losing hours of rest to late-night scrolling with measurable consequences for their mental health and academic performance.

“These spaces are just not made with children in mind. When a child goes on it and they just get sucked into the whole algorithm, the influence of marketing... the harm then outweighs the benefits.” Kids and Clicks

“One area that people don't think about is the screen time... what that actually means, both in a mental and physiological capacity... sleep deprivation, like how that has an impact on sleep patterns.” Why Sort It

“Algorithms are very capitalistic. Capitalism and algorithm it feeds on the negative... it realises there is engagement there.” Cake or Dice

An important and underappreciated theme emerging from this engagement is that the struggle for digital balance is not exclusive to children. Stakeholders note that adults are equally susceptible to addictive platform features, with many finding themselves 'sucked into the whole algorithm' alongside their children. This has significant implications. Adults who have not developed their own healthy relationship with technology are at a disadvantage to modelling or enforcing healthy digital habits for the young people in their care.

Recommendation for UK Government

- The Government is urged to recognise that social media is now an integral part of society and cannot simply be banned without addressing the underlying algorithmic architecture that prioritises engagement and profit over the safety and wellbeing of young users. Legislative action must address platform design, not just user behaviour.

Chapter 2: Interventions for safer, more positive experiences

- **What do you think the impacts would be of having a minimum age requirement higher than 13 for social media services?**

This was the most contested question amongst stakeholders. While the protective intention behind raising the minimum age for social media access is broadly supported, the practical implementation of a ban for those under 16 is viewed with deep scepticism by most contributors. The debate reveals a tension between the symbolic value of age thresholds and the practical realities of enforcement in a largely technically literate youth population.

Stakeholders are in broad agreement that technical enforcement of an age-based ban is, in its current form, nearly impossible. Young people are highly proficient at circumventing platform restrictions through tools such as VPNs and by misrepresenting their age during sign-up. The existing minimum age of 13 is widely acknowledged to be routinely ignored, with children as young as 8 or 9 accessing platforms designed for teenagers or adults.

Raising the threshold to 16 without a commensurate improvement in verification technology would, Stakeholders argue, produce the same outcome as a rule that exists on paper but has limited real-world effect. Critically, any age assurance system that relies on tech companies to self-police is viewed as fundamentally compromised.

“Bans are relying on effective age assurance technology... all of that can be sidestepped through a VPN. The conversation around bans is setting up a bit of a false promise.” **National organisation working on behalf of children and young people**

“It shouldn't always just fall on young people to be accountable for themselves when they're young people... how is Facebook, how are you guys actually being stricter to ensure that people aren't falling through the cracks?” **Scottish Scouts**

A significant and nuanced split exists across those interviewed regarding the psychological consequences of an outright ban. One school of thought holds that restricting access until age 16 would give children more time to develop their sense of self in the offline world, reducing peer pressure on parents and allowing for more gradual introduction to digital environments.

However, a compelling counterargument supported by several stakeholders warns of a 'forbidden fruit' effect. When young people are denied the opportunity to develop healthy digital habits in a safe, moderated environment during childhood, they may be ill-equipped to manage unrestricted access once they reach the legal age threshold. There are also practical concerns for older teenagers, a ban targeting under-16s would restrict 15-year-olds from accessing the digital networking tools increasingly essential for career development and further education applications.

“How will they learn to be responsible if they're not given a chance to learn how to be responsible in a safe environment...” **Scottish Scouts**

“To exclude your child from social media is to exclude them from an aspect of the world... By the age of 16, I feel like you've got a level of experience that could make you more responsible.” **MSYP**

“There seems to be a shift of responsibility on either the young people or the parents to safeguard. It's like no, what are you doing as the company?”
Sewing together All Nations

A significant and currently underexplored dimension of age assurance policy is its impact on adults, particularly those with lower levels of digital literacy, confidence, or access. While age verification mechanisms are primarily proposed as a tool to protect children, in practice they function as an access control system applied across the entire population. As such, they risk introducing new barriers that disproportionately affect adults who are already digitally excluded.

Evidence gathered through our stakeholder engagement, as well as our wider work on digital exclusion, indicates that many adults are already struggling to navigate existing digital systems, from configuring parental controls to understanding privacy settings. Even those who consider themselves digitally confident can find current systems to be complex, fragmented, and burdensome. The introduction of additional verification steps such as document uploads, biometric checks, or third-party authentication risks compounding this complexity and creating further points of disengagement.

These barriers are not evenly distributed. Older adults, kinship carers, people on low incomes, and those with limited digital skills are most likely to experience difficulty completing age verification processes. For some, these systems may prove functionally inaccessible due to a lack of appropriate devices, reliable

connectivity, or formal identification. For others, the barrier is psychological; stakeholders highlight that many adults feel embarrassment or stigma about gaps in their digital knowledge, which can deter them from seeking support when they encounter barriers.

There is a consequential risk that age verification requirements will lead not only to frustration but to exclusion. Adults may abandon processes they find confusing or intrusive, leading to reduced access to online spaces and services that are now integral to daily life, including communication, employment, education, and access to public services. This is particularly concerning given the increasing digitisation of essential services, where even small usability barriers can translate into significant real-world disadvantage.

Privacy and trust present an additional challenge. Our engagement demonstrates that many adults have limited understanding of how their personal data is collected, processed, and monetised online. Requiring these individuals to submit highly sensitive forms of identification, including biometric data, risks undermining trust further and may discourage engagement altogether. The individuals least confident in navigating digital systems are therefore those being asked to engage with the most complex and sensitive processes.

Taken together, these factors point to the need for a more holistic approach. Age verification cannot be considered solely through the lens of child protection; it must also be understood as a population-wide intervention with significant implications for adult inclusion, autonomy, and access. Without careful design, testing, and support, there is a real risk that measures intended to improve online safety will instead exacerbate digital exclusion among those already most at risk.

Recommendation for UK Government

- The Government must move beyond the 'false promise' of age-based bans. A more effective strategy would mandate robust, privacy-respecting age verification at the platform level.
- Hold tech companies legally accountable for enabling access by underage users.
- Invest in 'safety by design' standards that prevent harmful features from reaching young users in the first place.

- Take steps to review the need for further action around media literacy support for adults who are likely to be adversely impacted by additional age verification protocols.

Chapter 4: Preparing children for a digital future

Outside of schools, how could the UK Government better support children and young people to stay safe and feel supported online?

What should be considered when taking further action to support positive online spaces and content for young people?

Schools have historically been the default institution for delivering digital safety education. However, our engagement reveals strong and consistent evidence that this approach is no longer sufficient and that schools are too overstretched to carry this responsibility alone. Stakeholders call for a fundamental reorientation of where, how, and by whom online safety support is delivered.

There is broad consensus among stakeholders that third-sector organisations, charities, youth clubs, community groups, and national bodies play a vital role in delivering informal, trusted digital safety education. Several stakeholders made comment in relation to projects that complement and strengthen schools' efforts, particularly through support delivered outside the classroom environment. It was noted that effective support for children and young people whether in school or community settings is best achieved in partnership, with the third sector keenly aware of its own capacity limitations and therefore not positioning itself as a standalone solution.

The unique value in community settings lies in the relationships they foster. Youth workers and community leaders are perceived by young people as 'friends' rather than authority figures, enabling more honest and open conversations about risky online experiences.

Unlike schools, third-sector environments are not constrained by curriculum requirements, assessment pressures, or the power dynamics inherent in the teacher-pupil relationship. Children who might never disclose a concerning online experience to a teacher may feel entirely comfortable doing so in a youth club or community sports setting.

“That whole destination of an industry that supported young people outside the school is obviously challenged by resources. If you want it to happen, fund it.” **Seamab**

“We need to stop assuming that online safety is a school-only issue. Whether it's GPs, whether it's the local libraries, whether it's the youth club this is something that's integrated into our everyday life now.” **Kids and Clicks**

While there is strong agreement on the value of community-based support, stakeholders are divided on the optimal delivery model. Some advocate for high-level national public campaigns comparable to the anti-smoking or seatbelt campaigns of previous decades that create a shared cultural shift in how digital safety is discussed and understood across all age groups.

Others favour a more granular, 'place-based' approach embedding digital safety conversations into existing community infrastructure such as libraries, GP surgeries, leisure centres, and spaces where families already gather and where trust has been established over time. This approach recognises that a centralised campaign may not reach the families most in need of support.

“We need to adopt a wider public health approach that puts online health and harm on a par with public information campaigns around smoking and seatbelts.” **National organisation working on behalf of children and young people**

“The challenge the UK Government will have is they need to invest in youth work... but I do feel like that's where they need to invest.” **Why Sort It**

“If social media platforms were starting to be held accountable for stuff that happens... Because the platforms are not considered press, they're not held accountable. Where are the standards of that business?” **Cake or Dice**

The most urgent practical recommendation to emerge from this Chapter is the need for sustainable, multi-year funding for youth organisations. Stakeholders repeatedly note that the government cannot expect community and voluntary sector organisations to fill the gap left by platforms and schools without providing the resources to do so. Short-term project grants are inadequate meaningful digital safety work requires consistent staffing, long-term relationship-building, and access to up-to-date training and resources.



Recommendation for UK Government

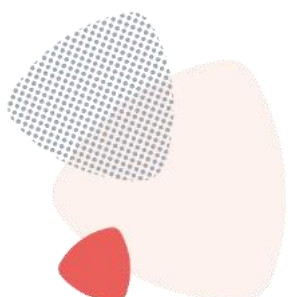
- Recognise that the ‘problem’ sits within telecommunications, a UK Government reserved function, but part of the solution is located within education and health, which are devolved competencies. A coordinated approach between the UK Government and the devolved administrations is required to
- Provide sustainable, multi-year funding to youth and third-sector organisations to deliver community-based digital safety education. Where UK Government allocates funding that is available in Scotland, either directly or through the Scottish Government, this should be compatible with ‘[Fair Funding](#)’.
- Coordinate a national public health campaign in collaboration with the devolved administrations, treating online harm with the same urgency as road safety or anti-smoking initiatives. Explore embedding digital safety support within NHS primary care settings, libraries, and community hubs.

Chapter 5: Supporting families

Many online platforms provide parental control tools which allow parents and carers to oversee and place parameters around children's online activity, including content, time, and functionality-based restrictions. How should this level of control change for children of different ages?

The question of parental controls sits at the intersection of child development, digital literacy, and corporate accountability. Stakeholders broadly support a graduated or ‘scaffolded’ approach to controls tightest in early childhood and gradually eased as young people develop the maturity and judgment to navigate digital environments more independently. However, the evidence also highlights deep concerns about the current model's fitness for purpose.

There is widespread agreement that parental controls should function as a teaching tool rather than purely a surveillance mechanism. The goal, stakeholders argue, should be to build trust, support the development of self-regulation, and give



young people the opportunity to make mistakes in a safe, supported environment rather than simply locking down access until a certain age.

Most stakeholders suggest that by the age of 16, young people should be treated with a degree of autonomy comparable to adults having been given the opportunity during their earlier years to develop responsible digital habits under appropriate supervision. The transition should be gradual and conversational, not a sudden lifting of all restrictions.

“When your child is still very young, putting those tools in place for boundaries... once they reach a certain age say 16 and above then that's it. You consider them as an adult.” **Kids and Clicks**

“Modelling behaviour is the most important thing I can do. As a parent I need to hold myself to the same standard I'm holding her to.” **Strange Town**

A recurring and significant debate with all stakeholders was whether parental controls should be calibrated to chronological age or to individual maturity. Stakeholders working with young people with additional support needs (ASN), neurodivergent children, or those in complex family circumstances emphasise that age alone is a blunt instrument. A child of 15 with significant additional support needs may require a level of digital protection more typically associated with a younger child, while a particularly mature 12-year-old might safely be given more independence.

This tension has implications for policy design as any age-based regulatory framework must build in flexibility for families and professionals to adjust controls based on individual developmental rather than applying a one-size-fits-all threshold.

“Thinking about ages and stages is important. An age doesn't need to define. You could have a really mature young person... but then you could have somebody the same age, but you're like, there's no way.” **Why Sort It**

“Is it a phone thing? Websites start being classified age-wise? Content starts being classified age-wise? But again, that would have to be a buy-in.” **Cake or Dice**

A theme running through all discussions on parental controls was the frustration at the current model, which places the entire burden of child protection on families rather than on the platforms that design and profit from the products children use. Stakeholders highlighted that the existing approach where parents must actively seek out and configure controls is the wrong way around. Platforms

should be 'safe by design', meaning that age-appropriate protections are the automatic default, not an optional extra buried in settings menus.

"We need to ask platforms to take a child safety by design approach building them in a way that doesn't include addictive features. There should be an equivalent of the child safety mark that's put on toys." **National organisation on behalf of children and young people**

"It should be the reverse way where I don't need to go to the settings. They're already in place for my child. It's safety by design in the first place." **Kids and Clicks**

Recommendation for UK Government

- Legislate to make 'safety by design' a mandatory standard for all platforms accessible to under-18s.
- Require that age-appropriate settings are automatically activated when a user's age is entered, rather than requiring parents to configure them manually.
- Introduce a child safety kitemark for platforms demonstrating compliance with design standards that protect young users.

Chapter 5: Supporting families

What would help parents and carers to more effectively use parental controls?

Our engagement paints a consistent and concerning picture of parents who are willing but overwhelmed. The current parental control ecosystem is fragmented, technically complex, often expensive, and poorly communicated. Rather than empowering parents, it frequently alienates them. Contributors are clear that the solution cannot be another PDF guide or a one-off training session. Sustainable, accessible, community-based support is urgently needed.

Stakeholders are united in identifying the complexity and fragmentation of existing parental control tools as the primary barrier to effective use. Rather than a single, unified point of control, parents must navigate separate settings at the router level, on each device, and within every individual application their child uses. A parent whose child plays a single video game may need to configure accounts and controls across multiple platforms simultaneously.

This technical burden described by contributors as navigating 'hoops' and 'layers of pages' is experienced as prohibitive even by parents who consider themselves digitally literate. For those with lower digital confidence, it can feel entirely insurmountable.

"I've got a house to run, I've got a job to do. When I was setting up my Xbox for my son, I had to set up a Unisoft account, an Unreal account... I don't have the inclination or the patience to be dealing with settings and stuff like that." **Sewing Together All Nations**

"We need very clear, easy-to-understand guidelines." **Seamab**

A significant and underappreciated divide exists around the cost of effective parental control tools. While free, basic controls are available, stakeholders note that the tools which work best are those that are genuinely robust and difficult for tech-savvy children to circumvent are typically available only through paid software subscriptions. For families on lower incomes, this creates a two-tier system in which protection becomes a privilege of wealth.

A separate concern relates to generational and cultural access. Kinship carers such as grandparents raising grandchildren may face a fundamental barrier of digital exclusion that no amount of simplified guidance can entirely bridge. Any government support strategy must account for this population explicitly.

"The more effective ones the ones that actually work they cost, and they're not cheap. Cost could be quite a large barrier." **Scottish Scouts**

"Adults might feel embarrassed to come forward. Age doesn't necessarily lead to that exact experience of knowing all these things." **MSYP**

"Sending them two-page PDF guides on how to do these settings just doesn't work. Tech companies have the ability to make these things a lot more simple than what they are right now." **Kids and Clicks**

Across all contributor groups, there is a compelling call to move away from static information products leaflets, PDF guides, one-off webinars towards long-term, community-embedded digital literacy support. The ideal model involves recurring, informal sessions in familiar settings such as youth clubs, libraries, school parent evenings, community centres, and healthcare settings such as GP surgeries. This will require coordination between UK Government, Scottish Government and local government.

These sessions should be delivered by trusted, knowledgeable facilitators and should acknowledge that many parents feel embarrassed about gaps in their digital knowledge. Creating a psychologically safe space for honest conversation is as important as the technical content itself.

Recommendation for UK Government

- Mandate that Internet Service Providers provide standardised, simple parental controls at the router level as a default and free-of-charge features.
- Fund long-term community training programmes not PDF guides that build genuine digital literacy for parents and carers of all backgrounds.
- Explore subsidised or free access to effective parental control software for low-income families.