Your response

Question 1: To assist us in categorising responses, please provide a description of your organisation, service or interest in protection of children online.
Is this a confidential response? (select as appropriate) No

Is this response confidential? – N

Carnegie UK's objective is better wellbeing for people in the UK and Ireland. Over the past three years, we have shaped the debate in the UK on reduction of online harm through the development of, and advocacy for, a proposal to introduce a statutory duty of care to reduce Online Harms. Our proposal is for social media companies to design and run safer systems – not for government to regulate individual pieces of content. Companies should take reasonable steps to prevent reasonably foreseeable harms that occur through the operation of their services (for example, the impact of recommender systems), enforced by a regulator.

The proposal has been developed by Professor Lorna Woods (Professor of Internet Law, University of Essex), William Perrin (Carnegie UK Trustee) and Maeve Walsh (Carnegie UK Associate). It draws on well-established legal concepts to set out a statutory duty of care backed by an independent regulator, with measuring, reporting and transparency obligations on the companies. Our way of working is to develop and publish detailed public policy proposals, drawing on our extensive legal, regulatory and policymaking expertise, for debate and adoption by others. For example, we published a draft Online Harms Bill to demonstrate that a systems-based regime is easy to legislate for.

Over the past two years, we have carried out work – in conjunction with a number of civil society organisations, academics and other expert groups – to develop principle-based model codes of practice that act at a systemic level to help tech companies assess and reduce the prevalence of online harm on their services. The work started with a code of practice on hate speech, which then informed ad hoc advice for the UN Special Rapporteur on Minority Issues. We then adapted this approach to produce – through the same collaborative process – a code of practice on online violence against women and girls and a draft of a code on mis/disinformation. We have recently used the learnings from these exercises to develop a model code for online harm reduction. We will refer to these examples throughout the rest of our submission, setting out both the principles that we feel online services should follow in addressing the particular functionality or design choice and, where relevant, extracting the subject-specific application of that principle from one or other or the published codes.

Question 2: Can you identify factors which might indicate that a service is likely to attract child users?
Is this a confidential response? (select as appropriate) No
We defer to organisations such as 5Rights Foundation who have done much work on the impact of design on children's engagement and experience online. From our own observations, which have informed our focus on systemic regulation, we would suggest the following factors would be in play: ○ A Service that is designed for access on mobile devices (smartphones, tablets, consoles etc) especially those recommended/rated as suitable for children via apps stores. ○ Services or apps that are heavily marketed at children via different media or host channels/accounts run by celebrities or prominent people who influence children. ○ Services that rely heavily on audio visual content – photos, videos, animations - and/or have functionality for users to create their own ○ Services with interactive functionality or where evidence suggests that they are being popularly used (like messaging apps) to run alongside child-dominated activities such as (online) gaming. ○ Younger children are likely to be drawn to services that promote animation/tie-ins with films, programmes, advertising; older children more via pop culture, celebrities, influencers, brands etc. ○ Services offering incentives for engagement – eg in-game rewards, likes, promotions, prizes. (See: the OFT's principles for Online and App-Based Games)

Question 3: What information do services have about the age of users on different platforms (including children)?
Is this a confidential response? (select as appropriate) No
Again, we would refer to the expert evidence of organisations such as 5 Rights and the AVPA. We would assume that the data and information collected by services to ensure they are compliant with the Children's Code (under the Data Protection Act) would be a useful benchmark. For instance, the Code sets out a non-exhaustive list, which we have extracted from below, including our own commentary in parentheses: ○ **Self-declaration** – This is where a user simply states their age but does not provide any evidence to confirm it … self-declaration of age can provide a useful starting point when providing privacy information and age-appropriate explanations of processing. ○ **Artificial intelligence** – It may be possible to make an estimate of a user's age by using artificial intelligence to analyse the way in which the user interacts with your service. Similarly you could use this type of profiling to check that the way a user interacts

Question 3: What information do services have about the age of users on different platforms (including children)?

with your service is consistent with their self-declared age. This technique will typically provide a greater level of certainty about the age of users with increased use of your service.

- **Third party age verification services** – You may choose to use a third-party service to provide you with an assurance of the age of your users. Such services typically work on an 'attribute' system where you request confirmation of a particular user attribute (in this case age or age range) and the service provides you with a 'yes' or 'no' answer. This method reduces the amount of personal data you need to collect yourself and may allow you to take advantage of technological expertise and latest developments in the field. If you use a third-party service you will need to carry out some due diligence checks to satisfy yourself that the level of certainty with which it confirms age is sufficient (PAS standard 1296 'Online age checking' may help you with this), and that it is compliant with data protection requirements. You should also provide your users with clear information about the service you use.
- **Account holder confirmation** - You may be able to rely upon confirmation of user age from an existing account holder who you know to be an adult. For example, if you provide a logged-in or subscription-based service, you may allow the main (confirmed adult) account holder to set up child profiles, restrict further access with a password or PIN, or simply confirm the age range of additional account users. [We would not here that this may be open to abuse by tech-literate teens who were seeking to avoid age restrictions.]
- **Social vouching**: Using a person's friends on social media to verify their age. The people who'll vouch for you need to have attained the minimum age set by the social media platform. You can ask up to three people to vouch for you before you're allowed access.
- **Technical measures** – Technical measures which discourage false declarations of age, or identify and close under age accounts, may be useful to support or strengthen self-declaration mechanisms. Examples include neutral presentation of age declaration screens (rather than nudging towards the selection of certain ages), or preventing users from immediately resubmitting a new age if they are denied access to your service when they first self-declare their age.
- **Hard identifiers** – You can confirm age using solutions which link back to formal identify documents or 'hard identifiers' such as a passport. However, we recommend that you avoid giving users no choice but to provide hard identifiers unless the risks inherent in your processing really warrant such an approach. This is because some children do not have access to formal identity documents and may have limited parental support, making it difficult for them to access age verified services at all, even if they are age appropriate. Requiring hard identifiers may also have a disproportionate impact on the privacy of adults.

Question 4: How can services ensure that children cannot access a service, or a part of it?

Is this a confidential response? (select as appropriate)

No

Question 4: How can services ensure that children cannot access a service, or a part of it?
In addition to following the guidance set out in our answer to question 3, we refer to some existing examples where services have developed forms of age assurance or age verification of users and other materials. For example, recent approaches by Instagram and Meta, while [Facebook Dating is using Yoti. We would observe here that some services, such as gambling sites or dating apps would require a more robust method of age verification than other services. We would also note, in relation to using third-party services, that there is a broader link here re companies' responsibilities in relation to their overall supply chain. We note also that TikTok has rules about amending birthdates and has published details of the platform's work on designing age-appropriate experiences. Beyond the platforms, the Australian e-safety commissioner has published guidance on how age verification shouldn't be "set and forget". The Children's Commissioner has also carried out work on age assurance, and Ofcom's own research shows how verification is very easily bypassed at the moment.

Question 5: What age assurance and age verification or related technologies are currently available to platforms to protect children from harmful content, and what is the impact and cost of using them?
Is this a confidential response? (select as appropriate) No
We believe this platforms and services are better placed to answer this.

Question 6: Can you provide any evidence relating to the presence of content that is harmful to children on user-to-user and search services?
Is this a confidential response? (select as appropriate) No

Question 6: Can you provide any evidence relating to the presence of content that is harmful to children on user-to-user and search services?

We assume that civil society organisations and charities such as NSPCC, Barnardos, Samaritans, Revealing Reality, 5 Rights, Molly Russell Foundation, Internet Matters, and others will be able to provide extensive evidence here. We very much support the position of 5 Rights this is not just about content: their work on the 4 Cs, including contact, conduct and contract as well as content is important. We have also, through the course of our work, argued that the precautionary principle is fundamental to designing regulatory approaches that adequately protect online users, particularly children, from harm: waiting to amass evidence of harm that is already occurring is too late and limiting approaches to preventing harm to that which is already evidenced will not mitigate the risk of future harm occurring on services.

Question 7: Can you provide any evidence relating to the impact on children from accessing content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

We defer to the organisations, such as those listed above, to provide the evidence here. However, we would also repeat the point made at the recent Ofcom roundtable discussion on this call for evidence that there is a "chicken and egg" scenario here whereby the questions ask specifically re encountering primary priority content and priority content. But a) those categories of content haven't been confirmed and are still subject to consultation prior to appearing in secondary legislation; b) they aren't themselves evidence-based. It would be helpful if Ofcom could clarify, in responding to this call for evidence, how they propose to use the research and evidence collected by this call that goes beyond that eventually designated as "primary priority" or "priority". This will be essential to provide further advice to companies and the government re the extent of harm that is likely to arise from non-designated content that falls beyond the final agreed lists and to consider how best this is mitigated.

There is an additional point to make with regard to the decision by the Government to remove the adult safety duties: childhood doesn't end at 18 and vulnerable teenagers/young adults will remain vulnerable. There are some serious considerations to be had re the effect of a "hard-stop" once users pass through the age barrier at 18, regardless of how effective AV or age assurance is.

Question 8: How do services currently assess the risk of harm to children in the UK from content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

Question 8: How do services currently assess the risk of harm to children in the UK from content that is harmful to them?

This is a question for services to respond to. We would, however, refer Ofcom to the principles we have set out in our recently published "Model Code" for regulatory approaches to social media. We refer in particular to Principle 1 (Responsibility, Risk Assessment, Mitigation and Remediation), which provides a generic approach to risk assessment that should be taken, not just relating to content that is harmful: the design and functionality of the service also needs to be taken into account. We have included the extract from the code below.

Principle 1: Responsibility, Risk Assessment, Mitigation and Remediation

1. The service provider must have a policy commitment to seek to reduce harm, whether in general or in relation to a set of harms, arising from the operation of their service endorsed by the board and significant subcontractors.
2. The governing board of the service provider should apply the United Nations Guiding Principles on Business and Human Rights, as should significant subcontractors in the supply chain. Large multinational service providers with complex supply chains should comply with the OECD Guidelines for Multinational Enterprises. Particular regard should be paid to risks of harm to media and democratic freedoms.
3. As a foundation for harm reduction activity, service providers must carry out a suitable and sufficient risk assessment of their entire service, including risks arising from the practice of outsourcing responsibilities. In doing so, service providers should engage with relevant experts and organisations representing groups adversely affected by operation of the service. A suitable risk assessment will follow international standards if available or best practice. It shall cover all territories where the service has a non-trivial user base, reflecting their local circumstances accordingly.
4. Where harm reduction is focussed on one or a few specific content domains (eg violence against women and girls), service providers should include a survey of the extent to which the relevant content domain arises and results in harm on its service.
5. Risk assessment must also be carried out in relation to the launch of any new service or new feature. Providers of high harm or very large services should operate a precautionary principle in introducing new features, only gradually increasing their availability while monitoring for harm in dialogue with representatives of victims.
6. The service provider must produce a risk mitigation plan addressing the issues raised in the risk assessment and at least covering the issues covered later in this code (including product testing).
7. The service provider must identify appropriate metrics to assess the appropriateness and success of the mitigation plan (or any part thereof) and use them to assess the effectiveness of the mitigation plan regularly (at least annually) and to update it as appropriate. Metrics should be designed so as to allow comparability across assessment periods.
8. The service provider must remain vigilant at all times to reasonably foreseeable events that could give rise to significant harm such as elections, festivals, sports matches etc or observable yet unforeseen events such as civil unrest, war or severe ethnic tensions and mitigate the harm arising from their services in these contexts. Advances in technology leading to or exacerbating harm will occur and should be mitigated as part of ongoing vigilance. In general the service provider should review the success of the mitigation plan at least annually and revise the plan as appropriate.
9. In reviewing progress, service providers must engage with relevant experts and organisations representing groups adversely affected by the relevant content.
10. Risk assessments and mitigation plans should be recorded, retained for not less than three years and published on the service provider's website in an accessible manner in languages

Question 8: How do services currently assess the risk of harm to children in the UK from content that is harmful to them?
commonly used on the service. The service provider should consider instructing third party audits from independent appropriately qualified auditors. 11. Risks assessments should not assume that users and the way they respond to the service and the content on the service are homogenous. Risk assessments must take into account the characteristics of different groups and the differential impact of the features on them as well as the specific risk of harm to which they are exposed. Specifically, harms arising for children should have a separate risk assessment and mitigation process, informed by General Comment No. 25 of the UN Committee on the Rights of the Child in relation to the digital environment. 12. This first principle is a foundation for principles 2-12. The following principles are applied with reference to assessing and mitigating risk arising from the operation of the services, in all non-trivial geographic markets and including the actions of significant sub-contractors.

Question 9: What are the exacerbating risk factors services do or should consider which may have an impact on the risk of harm to children in the UK?
Is this a confidential response? (select as appropriate) No
n/a

Question 10: What are the governance, accountability and decision-making structures for child user and platform safety?
Is this a confidential response? (select as appropriate) No
It is important that systems should appropriately differentiate between groups that have specific vulnerabilities (with particular regard for intersectional groups); that there should be appropriately trained staff; staffing should be sufficient; adequate provision of support to users - consult not just representatives of children's lobby but find some way to engage with children too; have processes that can identify specialist children's issues from general operating issues and get appropriate teams involved. From a governance perspective, it is important that responsibility for children's well-being is accepted at Board level.

Question 11: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements for children (including children of different ages)?
Is this a confidential response? (select as appropriate) No
We would refer to the work done previously by Children's Commissioner and by 5 Rights on child-friendly, accessible terms of service. In our submission to the call for evidence on illegal content, we referred to the code we had developed on violence against women and girls. We have further developed that model in recent months to inform our recently published "Model Code" for regulatory approaches to social media. We refer in particular to Principle 5 (Access to the Service), where we suggest that; "*The service provider must make its terms of service (including any privacy policy) and/or community standards visible to would-be users and advertisers before they sign up to the service. The terms of service and/or community standards must be expressed in clear and easy to understand language bearing in mind the comprehension capabilities of groups likely to use the service. This includes providing different language versions of the terms of service and/or community standards appropriate to the territories in which the service is made available. The service provider should have in place expanded guidance explaining their terms of service/privacy policies/community standards (and how these are developed, enforced and reviewed, plus the role of relevant survivors' groups and civil society in developing them). It should ensure that training and awareness tools are readily available to users on the Terms of Service and Community Guidelines to ensure users are aware of permitted content and behaviours on the platforms*."

Question 12: How do terms of service or public policy statements treat 'primary priority' and 'priority' harmful content?[1]
Is this a confidential response? (select as appropriate) No
We defer here to the submissions that will be made from service providers and to publicly available information. We would however also make the point here that the Government's decision to weaken the duties with regard to content that is harmful to adults lays open the possibility that services may weaken existing ToS and public policy statements with regards to adult users which could well have a knock-on impact on the assumed protections that these also give to children.

[1] See A1.2 to A1.3 of the call for evidence for more information on the indicative list of harms to children.

Question 13: What can providers of online services do to enhance children's accessibility and awareness of reporting and complaints mechanisms?
Is this a confidential response? (select as appropriate) No
In our submission to the call for evidence on illegal content, we referred to the code we had developed on violence against women and girls. We have further developed that model in recent months to inform our recently published "Model Code" for regulatory approaches to social media. We refer in particular to Principle 11 (Reporting and Complaints) where we suggest that: *1. The service provider must have reporting processes that are fit for purpose, that are clear, visible and easy to use and age-appropriate in design and cover all content and behaviour (whether user-generated, service generated (eg autocompletes) or advertising-based). A service provider should consider whether some forms of complaint (eg harassment; image-based sexual abuse) need specially designed reporting processes.* *2. The service provider should allow users and others to complain about unsafe design features that are not 'content'.* *3. The service provider must provide the opportunity for non-users who are affected by content or behaviour on the service to report that content and/or behaviour* *4. A service provider should record complaints in a sufficiently granular manner to feed into risk assessment review processes. The typology should be developed with survivor representatives.*

Question 14: Can you provide any evidence or information about the best practices for accurate reporting and/or complaints mechanisms in place for legal content that is harmful to children, or users who post this content, and how these processes are designed and maintained?
Is this a confidential response? (select as appropriate) No
n/a

Question 15: What actions do or should services take in response to reports or complaints about online content harmful to children (including complaints from children)?
Is this a confidential response? (select as appropriate) No
See above. Evidence over a number of years from organisations that support children who have experienced online harms, or from surveys of children and young people, suggests that children often do not report having been harmed because (a) nothing happened; or (b) they didn't know what was happening. So it is important that people who raise reports or complaints are told what's going on and that this shouldn't be just an automated one off message but about progress, what the decision was and why and how to appeal - and all in age appropriate language. It is also worth considering to what extent should responsible adults be able to complain on behalf of children (especially young ones).

Question 16: What functionalities or features currently exist that are designed to prevent or mitigate the risk or impact of content that is harmful to children? A1.21 in the call for evidence provides some examples of functionalities.
Is this a confidential response? (select as appropriate) *[Please select]*
We refer Ofcom to our previous submission on the call for evidence on illegal content.

Question 17: To what extent does or can a service adopt functionalities or features, designed to mitigate the risk or impact of content that is harmful to children on that service?
Is this a confidential response? (select as appropriate) *[Please select]*

Question 17: To what extent does or can a service adopt functionalities or features, designed to mitigate the risk or impact of content that is harmful to children on that service?
n/a

Question 18: How can services support the safety and wellbeing of UK child users as regards to content that is harmful to them?
Is this a confidential response? (select as appropriate) *[Please select]*
n/a

Question 19: With reference to content that is harmful to children, how can a service mitigate any risks to children posed by the design of algorithms that support the function of the service (e.g. search engines, or social and content recommender systems)?
Is this a confidential response? (select as appropriate) No
In our submission to the call for evidence on illegal content, we referred to the code we had developed on violence against women and girls. We have further developed that model in recent months to inform our recently published "Model Code" for regulatory approaches to social media. We refer in particular to Principle 7 (Discovery) where we suggest that: *1. The service provider should review their recommender systems, whether in relation to content or to other users to follow, especially their automated systems, so they do not promote harmful content in general or that related to a specific content domain identified as problematic. The service provider should check automated systems for bias (e.g. arising from training data). The service provider should consider the risks of tools/features used for organising content (eg hashtags) and what safeguards should surround their use, for example to prevent terms inciting violence against minoritised groups being used.*

Question 19: With reference to content that is harmful to children, how can a service mitigate any risks to children posed by the design of algorithms that support the function of the service (e.g. search engines, or social and content recommender systems)?

2. The service provider should consider the impact of autoplay functions, especially in the context of content curated or recommended by the provider. When a service provider seeks to take control of content input away from the person in this way the provider should consider how this feature might affect a person's right to receive or impart ideas.
3. The service provider should consider whether to provide appropriate information to its users about the accuracy (or otherwise) of information (eg flagging content that has been fact-checked) and should make its policies in this regard available.
4. The service provider must consider how its advertising delivery systems affect content seen by users. In particular, it must consider the circumstances in which targeted advertising may be used and managerial oversight over the characteristics by which audiences are segmented where those segments might be computer or user - generated.
5. The service provider must have terms of service and/or community standards in respect of its advertisers that are fit for purpose taken against its values, local laws and international human rights and should have processes in place to enforce that policy consistently.
6. The service provider must consider the need for explainability or interpretability, accountability and auditability in designing AI/ML systems.
7. For users who are children, the service provider should ensure that Principle 7 is applied to reflect their particular characteristics and vulnerabilities, including their right not to see some information.

Question 20: Could improvements be made to content moderation to deliver greater protection for children, without unduly restricting user activity? If so, what?

Is this a confidential response? (select as appropriate)

No

In our submission to the call for evidence on illegal content, we referred to the code we had developed on violence against women and girls. We have further developed that model in recent months to inform our recently published "Model Code" for regulatory approaches to social media. We refer in particular to Principle 12 (Moderation) where we suggest that:

1. The service provider's policies must be effectively and consistently enforced in accordance with its detailed policies and further guidance. Such further guidance must be in accordance with national law and international human rights.
2. The service provider must have in place sufficient numbers of moderators, proportionate to the service provider size and growth and to the risk of harm, who are appropriately trained to review harmful and illegal content and who are themselves appropriately supported and safeguarded.
3. Where automated tools are used, the service provider must put in place processes to ensure those tools operate in a non-discriminatory manner and that they are designed in such a way that their decisions are explainable and auditable. Users should be informed of

Question 20: Could improvements be made to content moderation to deliver greater protection for children, without unduly restricting user activity? If so, what?

the use of such tools. Machine learning and artificial intelligence tools cannot wholly replace human review and oversight.

4. The service provider must establish clear timeframes or other benchmarks for action against non-compliant content.

5. Action in relation to a complaint must be proportionate to the severity of the harm likely to be caused; content contrary to the criminal law is to be dealt with swiftly. The terms of service should make clearly the nature of any such action and the circumstances in which it would arise, as well as details of any appeals process. Action could include:

> *a) Label content as inaccurate/misleading; b) Demonetise content; c) Suppress content in recommender tools and/or search engines; d) Geo-blocking of content; e) Suspension of content; f) Removal of content; g) Non-recommendation of user and/or group as person to follow; h) The existence of a strike system; i) Geo-blocking of account; j) Suspension of account; k) Termination of account.*

6. The service provider should have systems of assessment and feedback to the initial reporter and the owner of content that has been flagged and actioned to ensure transparency of decision making. Users should be kept up to date with the progress of their reports and receive clear explanations of decisions taken.

7. The service provider should consider the risk of abuse of complaints processes and put in place appropriate safeguards. It should put in place a right of appeal on all decisions made concerning illegal or harmful content, or content that has been flagged as illegal or harmful content. This system cannot displace user rights to take action before the courts. All users must be given a right to appeal any measures taken against them, whether in full or in part. Users must be able to present information to advocate their position.

8. The service provider should have appeals systems which must take no longer than seven days to assess appeals, except in exceptional circumstances which are unforeseeable and beyond the provider's control (see Principle One for discussion of foreseeable events – such as elections – and unforeseeable ones – such as a war).

9. The social media provider must consider putting in place an appropriately knowledgeable and independent trusted flagger programme that maintains its independence from the service provider and from governments. The service provider should:

> *a) ensure trusted flaggers are not used as a sole provider of flagging content; b) ensure trusted flaggers are appropriately compensated, while not compromising their independence; c) hold regular meetings with members of the trusted flagger programmes to review content decisions and discuss any concerns; d) provide support to trusted flaggers who are exposed to harmful content in line with the service provider's support to its own moderation teams. e) The service provider should have a crisis response protocol that plans for crises of different types in general and, for foreseeable crisis-types, has methodologies to enable the continued delivery of the service without causing harm in accordance with international best practice. This should include occasions when a government seeks to exert undue influence. All protocols should be drafted in clear and precise language. These protocols should include conflict affected and high risk areas, and processes for identifying and monitoring such areas based on existing classifications (eg OECD States of Fragility) as well as monitoring statements from bodies such as the UN or the International Red Cross. Protocols should be tested before deployment and regularly audited in operation.*

Question 20: Could improvements be made to content moderation to deliver greater protection for children, without unduly restricting user activity? If so, what?
We would also note that it is important to have appropriately drafted Terms of Service that reflect the harms on the platform - and that those ToS are drafted in sufficiently granular terms. We would also distinguish between pre-moderation (upload filters) and post-moderation (own initiative review as well as response to complaints). Finally, it may be worth probing whether automated content moderation systems trained on mainly adult data work for children.

Question 21: What automated, or partially automated, moderation systems are currently available (or in development) for content that is harmful to children?
Is this a confidential response? (select as appropriate) *[Please select]*
n/a

Question 22: How are human moderators used to identify and assess content that is harmful to children?
Is this a confidential response? (select as appropriate) *[Please select]*
n/a

Question 23: What training and support is or should be provided to moderators?
Is this a confidential response? (select as appropriate) *[Please select]*

Question 23: What training and support is or should be provided to moderators?
n/a

Question 24: How do human moderators and automated systems work together, and what is their relative scale? How should services guard against automation bias?
Is this a confidential response? (select as appropriate) *[Please select]*
n/a

Question 25: In what instances is content that is harmful to children, that is in contravention of terms and conditions, removed from a service or the part of a service that children can access?
Is this a confidential response? (select as appropriate) *[Please select]*
n/a

Question 26: What other mitigations do services currently have to protect children from harmful content?
Is this a confidential response? (select as appropriate) *[Please select]*
n/a

Question 27: Where children attempt to circumvent mitigations in place on a service, what further systems and processes can a service put in place to protect children?
Is this a confidential response? (select as appropriate) *[Please select]*
n/a

Question 28: Other than those covered above in this document (the call for evidence), are you aware of other measures available for mitigating the risk, and impact of, harm from content that is harmful to children?
Is this a confidential response? (select as appropriate) No
We would recommend that it is important that the platform is able to point children to support services, in the event that they experience harm; and to consider to what extent parents or guardians should be involved. We would also consider it important that they have crisis protocols for events where individual children are found to be at risk of, or in imminent danger.