Ofcom Online Safety Team
Ofcom
Riverside House
2A Southwark Bridge Road
London
SE1 9HA
protectingchildren@ofcom.org.uk

July 17, 2024

Re: Protecting children from harms online

Bandio appreciates the opportunity to comment on the Office of Communication ('Ofcom')
consultation ('the Proposal') on the UK Online Safety Act 2023 ('the Act').

Bandio is a public benefit corporation that was started by Common Sense and a leading
cryptography and blockchain organisation, Aleo Networks Foundation. Bandio was created to
provide a privacy-preserving solution to age assurance that is parent and youth friendly. We
believe our technology can play a critical role in the future of online safety for children and
families.

About Bandio

The lack of age appropriate access online is a pervasive and a growing problem for platforms
and parents; and current platform-built solutions simply don't work. Bandio wants to see Ofcom
craft rules that recognize privacy-preserving technologies, like zero-knowledge proofs and
related cryptographic solutions, as preferred solutions for protecting consumers and their
privacy. A failure to do so will only perpetuate the status quo, which undermines consumer
safety, privacy and trust.

Bandio has developed a solution which gives parents a way to make sure that their child or teen
isn't wandering the digital world as an adult by providing age verification which is convenient,
secure, and private. Bandio is like the anonymous colour-coded wristbands you get at a theme
park or a festival. You flash your ID once at the entrance, and then all the vendors can verify
your age range without asking for your ID again. Further, by utilising privacy-preserving
technologies, we avoid retaining any personal data. Because Bandio doesn't retain any
identifying information such as an email address, there is no risk of creating a "honeypot" for
hackers and no risk of personal identifying data being used by entities for purposes not
permissioned by users. Bandio allows organisations to confirm a user's age range without
knowing, capturing, or retaining any sensitive information beyond the user's age range.

Bandio is responding to this consultation because we believe that our approach to age
assurance and parental consent offers a set of desirable characteristics, some of which became

possible only recently due to technological advancements with zero-knowledge proofs, which is privacy-preserving technology that more companies are beginning to leverage. A few important aspects of our product are:

- Trusted third party - Bandio is Common Sense Media's solution, and we are able to complement the trusted information that Common Sense provides parents and families.
- Interoperability - The age estimation or verification process results in a reusable 'age band' that can be used across participating sites and apps.
- Privacy-protective - users can provide their age range at participating sites and apps without providing any other personal identifying information, and yet the sites and apps can still verify the validity of the age band.
- Ease of use for parents/guardians/families - Parents can create age bands for their kids and younger teens and, in the future, where needed for individual platforms, provide consent all in one place.
- Limited data use - Personal identifying information is not used for any purpose other than verifying age and is discarded immediately after age is confirmed.
- No data retention - No personal identifying information is retained after age estimation or verification.
- Distributed networking - No centralised collection of age bands is created, so there is no attractive target for hackers.

Our consultation response

Volume 2: Do you agree with our proposals in relation to children's access assessments (Section 4)?

Bandio is highly supportive of Ofcom's proposals that service providers should only conclude that children are not normally able to access a service when the service providers are using highly effective age assurance. Further, we are supportive of the four proposed criteria of technical accuracy, robustness, reliability and fairness.

As Bandio is an age assurance technology that would be classified as 'highly effective', we believe that technical accuracy and robustness of the verification process needs to be balanced against proportionality. A service provider could, for example, ask for many different types of documentation and evidence as part of the age assurance process to ensure that the end result is 'robust' and 'accurate'. However, this could cause excessive friction, resulting in customers using other service providers (which may not be 'highly effective') or looking to obfuscate the process through workarounds; an issue which is already recognised in the Proposal as a problem. Further, and perhaps more worrying, service providers collecting and storing excessive amounts of personal information only creates a target for hackers.

We therefore encourage Ofcom to contemplate introducing a fifth criteria around data proportionality, which looks to ensure that the use of highly effective age assurance techniques becomes widespread because they are convenient and user friendly.

Further, to ensure that a security risk is not inadvertently created by incentivising excessive data collection, we encourage Ofcom to make it clear that any personally identifying data collected for the purposes of age assurance must be deleted immediately and not used for any other purpose beyond confirming a user's age range.

Regarding the proposed interpretation of "significant number of users who are children", we agree with Ofcom's approach, and understand the policy rationale behind not wishing to provide numbers, as such numbers are highly context specific and may result in services that potentially pose a very serious risk of harm to a relatively small number of children concluding that they are not in scope of the child safety duties. However, we believe it may be helpful to provide:
- Case study examples on both ends of the spectrum: where objectively a low number of users are children, but the context risks are high enough for Ofcom to consider the number 'significant'; and the reverse, i.e. a larger number of children but representing very low context risk and the conditions under which Ofcom would not consider this to be significant.
- Examples of context risks that Ofcom would consider so high as to result in <u>any</u> number of child users to be significant.

<u>Volume 3 Do you have any views on Ofcom's assessment of the causes and impacts of online harms (section 7)?</u>

Bandio notes Ofcom's proposal to introduce five age categories based on a number of developmental and life stage factors, as well as changes in parental supervision. While we agree broadly with this categorisation, we encourage Ofcom to further consider and stratify the 6-12 age band from two to three.

Bandio has done this in our age assurance solution based on evidence from our partner, Common Sense Media, regarding the changes children experience both developmentally and socially during this time window. [Common Sense Media](#) combines original research with a number of different child content inputs - including movies, TV shows, podcasts and books - to create a more bespoke, independent age rating system that supports families as they navigate the challenges and possibilities of raising children in the digital age.

We found that the difference between a six year old, a nine year old and a 12 year old are marked enough to warrant them being three categories rather than two (for example, Bandio has 6-8, 9-10 and 11-12).

We also note paragraph 7.11.3 "*Device-sharing between children and adults may lead to a risk of a child being recommended age-inappropriate or harmful content*". While we acknowledge that this is certainly a risk, there are ways of mitigating this. For example, Bandio allows you to create multiple age bands on the same device. The device will assume the youngest user is operating the device, unless the user selects an older age band (which we recommend be set up with a password so as to avoid easy use by younger members of the family). It is therefore very possible for service providers to utilise highly effective age assurance techniques while also

minimising the risks associated with device sharing. We therefore encourage Ofcom to draft policies accordingly and ensure service providers are operating at the highest standard possible.

<u>Volume 4: How should services assess the risk of online harms? Children's Risk Assessment Guidance and Children's Risk Profiles' (Section 12)</u>

Overall, Bandio agrees with Ofcom's proposals in relation to the Children's Risk Assessment Guidance and the four step risk assessment process.

However, as a general point we would like to see Ofcom strengthening the expected role of age assurance, in particular highly effective age assurance techniques. Such techniques are absolutely crucial to ensuring the protection of children and young people online, and Ofcom can only deliver its desired policy outcomes by embracing and fully supporting age assurance. It is simply unacceptable for service providers to claim that implementing robust processes are too complicated or expensive; service providers have a moral obligation to protect the children who access them and this can only be possible by implementing the highest possible standards.

Bandio therefore believes that the guidance, insofar as it is supportive of the Act, should require the implementation of highly effective age assurance processes unless there is clear evidence to support why this is not practical/possible. We note that paragraph 4.47 states "We expect many service providers to be unable to distinguish users of different ages (including differentiating children from adults; or children within different age groups) to a high level of confidence." We highly refute this statement - technology solutions like Bandio exist which are both robust and cost effective. While we appreciate that Ofcom is trying to strike a balance of proportionality with industry, we are concerned that statements like this will be used by some service providers as the excuse they need not to take age assurance seriously and not to implement the highest possible standards. Instead, we would encourage Ofcom to shift the burden of responsibility back onto service providers and expect that wherever practical, they should utilise highly effective age assurance technologies to distinguish children from adults, and different categories of child.

Further, requiring highly effective age assurance techniques wherever practicable in step 2, will only serve to enhance the effectiveness of steps 3 and 4. By fully understanding the age classifications of users, it is much easier to design and implement targeted interventions which can be reviewed and further developed over time.

<u>Volume 5 – What should services do to mitigate the risk of online harms</u>

Our proposals for the Children's Safety Codes (Section 13)
- Bandio is highly supportive of the safety code proposals, and applauds Ofcom for such thoughtful and robust implementation of highly effective age assurance techniques.
- As with our previous comments, our main recommendation here is for Ofcom to continue to strengthen its expectation around the use of age assurance wherever possible. For

example, making it clear that service providers are expected to use highly effective age assurance techniques unless there is justifiable and reportable reasons why they can't (rather than the expectation being 'a greater use of').

Developing the Children's Safety Codes: Our framework (Section 14)
- Bandio is similarly highly supportive of the safety code framework.
- In particular, in relation to Q27 (Do you agree that most measures should apply to services that are either large services or smaller services that present a medium or high level of risk to children) we would like to highlight our support for this proposal.

Age assurance measures (Section 15)
- Bandio is generally supportive of the measures outlined in section 15, however we have some specific comments outlined below.
- We appreciate that Ofcom does not want to recommend specific age assurance methods in its measures, and indeed, supporting any particular business could be considered anti-competitive. However, we do note that there is precedent for regulators to maintain a list of the types of technologies that they would consider appropriate for meeting a particular requirement, or indeed technologies that would likely be inappropriate. So for example, we would not expect Ofcom to endorse a firm like Bandio, but it could say that highly effective age assurance measures utilising zero knowledge proof technology could meet the criteria of technical accuracy, robustness, reliability and fairness.
- While we note such an approach would need to be evolved over time, it would be helpful clarification for service providers, and would help reinforce expectations of Ofcom.
- Finally, in relation to Q32 (Do you agree with our proposal to recommend the use of highly effective age assurance to support Measures AA1-6) we would like to highlight our support for this proposal.

Search moderation (Section 17)
- Bandio notes paragraph 17.7 in particular:
  - *We note that for U2U services, the Act requires certain services to use highly effective age assurance to prevent children from accessing PPC. The Act, however, does not require search services to use age assurance technologies to comply with the children's safety duties. Though it is something we may consider in the future, at this stage, we do not consider it proportionate to recommend that search services implement any form of age assurance to directly target their moderation actions to child users.*
- We do not think it would be disproportionate for search engines to default to "appropriate for < 13 year olds" and for users who can demonstrate they are 13+ can get access to the full search engine functionality.

*   *   *

Finally, we would like to reiterate the importance of privacy preserving technologies in delivering age assurance. The ICO's Children's Code on the processing of children's personal data reiterates the UK GDPR seven key principles which lie at the heart of data protection. Data storage is a crucial aspect of data processing, and in line with the principles of data minimisation and storage limitation, supporting technologies which don't require the storing of personal data, like zero knowledge proofs, is a key way to support these principles.

We accordingly urge Ofcom to craft rules that recognize privacy-preserving technologies, like zero-knowledge proofs and related cryptographic solutions, as preferred solutions for protecting consumers and their privacy. A failure to do so will only perpetuate the status quo, which undermines consumer safety, privacy and trust. Emerging products like Bandio meet all of these characteristics, and provide a feasible and practical solution for companies who need reliable age range information.

We are happy to have follow-up conversations, and discuss more with you about Bandio's solution.