MEDIERÅDET
FOR BØRN & UNGE

The Media Council for Children and Young People's ethical guidelines for digital service providers

Children and young people are entitled to have the best conditions to participate in the digital environment safely, age-appropriately, and in accordance with their rights. Children are particularly vulnerable and exposed to the risks posed by digital services - including harmful and illegal content, subliminal marketing, grooming, radicalization, and much more. Many digital services use opaque designs and business models based on offering a free product in exchange for collecting and selling information about their users. This exposes children to risks to their right to privacy and impairs their ability to make choices based on their own needs and desires. Specifically, it manifests itself through unclear retention mechanisms and other behavioral designs that maximize user engagement among children and young people.

Therefore, The Media Council for Children and Young People has drafted a set of ethical guidelines that digital services must comply with if they want to protect children in the best possible way. Any digital service intended for or accessed by children should be designed with respect for children's rights.[1] Ensuring the rights and needs of children is paramount, hence, digital service providers will need to restructure their designs to put the best interests of children first.

Children's digital rights are defined in a number of codes, laws, and conventions that can be difficult to navigate due to their volume. The ethical guidelines are based on children's rights as enshrined in the UN Convention on the Rights of the Child, with inspiration from the EU BIK+ Strategy, GDPR, Age Appropriate Design Code (AADC), Digital Services Act (DSA), and the AVMS Directive.

These ethical guidelines should be seen as comprehensive and complementary to the aforementioned legal acts and international conventions, with a focus on supporting the best interests of the child.

Purpose:

The Media Council's ethical guidelines contain a number of principles for design, operation, and user interface that digital service providers must comply with to meet their responsibility for ensuring that children and young people have the best conditions for participating in the digital environment safely, age-appropriately and in accordance with their rights. The guidelines have been developed in cooperation with a number of relevant actors in the field.

The ethical guidelines for digital service providers serve three purposes:

- Recommendations for digital service providers' best practices and design with a focus on the best interests of the child.
- Education for society and consumers that increases knowledge about the best interests of the child in digital environments and thus improves the ability to regulate and act on it.
- A basis for labeling the digital service providers' compliance with the ethical guidelines, so that children and parents know the risks and degree of safety for children using the service.

[1] Children are defined as people under 18 years of age, cf. the UN Convention on the Rights of the Child and its addendum General Comment 25 (2021).

Who are the guidelines for?

All providers of digital services accessed by children and young people should adhere to the ethical guidelines. The guidelines are aimed at and developed with a focus on online platforms often referred to as 'social media', which offer visitors the possibility to create and explore profiles and share content.

The ethical guidelines are also intended for digital gaming services in instances where digital games and gaming platforms have the character of social media by allowing message sharing, exploring other players' profiles, etc. These services form an increasingly large part of children's digital use and it is important that they are safe, age-appropriate, and in line with children's rights.

The ethical guidelines apply to both Danish and international services that are accessed by children under the age of 18. Many services have age limits of 13 years. However, this age limit can easily be circumvented in practice due to a current lack of verification. Having an age limit does not exempt services from responsibility if there are users under this age using the service. The Media Council for Children and Young People in Denmark encourages all Danish or global digital service providers whose service is intended for or accessed by children to assess, adjust, and develop their service in accordance with these guidelines.

Ethical guidelines for digital service providers

The following section presents the Media Council for Children and Young People's ethical guidelines for digital services.

1. The platform must be designed in the best interest of the child[2]

1.1 Digital service providers must design their services with the best interests of the child[3] as a primary consideration if they are intended for or can be accessed by children.

1.1.1. Consideration of the best interests of the child means that the service provider designs, operates, and continuously adapts its service with respect for the rights of the child in the digital environment and takes into account the best interests of children, including their cognitive and emotional development.

1.1.2. Children, young people, and parents must be continuously involved in the adaptation of the service. This applies to design, development, and ongoing evaluation.

2. Terms of use and service must be understandable to children

2.1. The service provider must balance terms of use and terms of service with fundamental rights and communicate them and other information to users in concise, accurate, and clear language and in formats that support the child's understanding.

2.2. The service provider must assess the risks pertaining to its service and provide information about the risks associated with the service that may violate the rights of the child, cf. section 1, and in accordance with the instructions mentioned in section 2.1. The service provider must also mitigate and address these risks and document how they are addressed.

2.3. The service provider must have guidelines for communication between users and content sharing on the service and support compliance by users in order to prevent and counteract illegal and potentially

[2],[3] The best interest of the child is synonymous with the welfare of the child and means an assessment and prioritization of what is best/most beneficial for the child.

harmful practices, such as but not limited to discrimination, threats, sharing of offensive content, scamming and fraud, bullying, grooming, encouraging self-harming behavior, and spreading misinformation.

2.3.1. Support for users' compliance with the guidelines must not lead to inappropriate monitoring of and data collection about users, cf. section 3. The support may, for example, consist of measures that ensure users' knowledge and understanding of the guidelines.

3. Use of children's data must be minimized and in the best interest of the child

3.1. The service must by default have the highest level of privacy. This entails that by default the use of children's data is limited to what is essential for the functioning of the service. The collection and processing of personal data about children for commercial use must be excluded. This applies, for example, for marketing and profiling purposes. Data collection and processing that does not have the best interests of the child as a primary consideration must be excluded. The service provider must also document how they comply with data responsibility and data minimization, cf. the basic principles of the GDPR[4].

3.1.1. Consent to data collection and processing must only be given freely and on an informed basis and must otherwise comply with the conditions for valid consent under the GDPR. The service provider must communicate in an age-appropriate manner and ensure that the child understands what personal data is collected, for what purpose, how it is processed, and what consequences it may have for the child.

3.1.2. The service provider must only share data about a child if it is strictly necessary to safeguard the best interests of the child and/or important public interests, which excludes data sharing for commercial reasons, cf. 3.1. Any sharing of data about a child must be justified.

3.1.3. The possibility for the child/parent to change the default settings, cf. section 3.1, must be weighed against the best interests and rights of the child. If the child changes a setting, such as enabling geolocation, the change must, as far as possible, only apply to the child's current session. The service provider must inform the child/parent of the consequences the change may have and communicate this in accordance with the principles in section 2.1.

4. Children should not be able to access harmful and illegal content

4.1. In order to take into account the best interests of the child, cf. section 1, and in light of the risk assessment that must take place in accordance with section 2.2, the service provider must ensure that illegal content and content that may seriously impair children's development cannot be accessed by children. Other content must be adapted to the child's age and development, cf. section 1.1.1, based on an assessment of the content's potential harm and taking into account the child's freedom of expression and information.

4.1.1. When assessing content, the service provider must consider the context in which the content is included.

4.1.2. The service provider must establish and maintain systems that enable children to determine the origin and authenticity of content.

[4] Cf. Article 5 and the principles for processing personal data.

Age verification must be effective and user-friendly
4.2. The service provider must establish and maintain effective, user-friendly, and privacy-protective systems for age verification of users accessing the service. These systems can beneficially be managed by an independent third party that complies with the principles in section 3.

4.2.1. To ensure that the service is age-appropriate, the service provider must design, continuously assess, and adapt the service based on the child's age and cognitive and emotional development.

4.2.2. The age limit of the service must reflect a general consideration for children's protection and use, including personal data protection and freedom of expression and information.

4.2.3. The service provider must ensure that the age limit and target group of the service are clear and justified for children and adults, cf. section 2.1.

4.2.4. The service provider must ensure that children who meet the age limit can access and use the service in accordance with the requirements mentioned in section 1.1.1.

5. Easy reporting of harmful and illegal content
5.1. The service provider must clarify where users, regardless of whether they are registered users of the service, can report content and incidents that are illegal or are considered likely to harm children. The service provider must ensure that the reporting process is efficient, user-friendly, and transparent, thereby facilitating the submission of sufficiently accurate and substantiated reports. The service provider must also proactively take appropriate measures to minimize the occurrence of illegal and harmful content and incidents on their service.

5.1.1. Upon notification of illegal and/or harmful content, the service provider must immediately decide whether the content should be removed or blocked. The service provider must ensure the necessary documentation upon notification and without undue delay inform the parties involved of the possibilities of appeal.

5.1.2. If content is removed or blocked, the notifier and the user whose content is removed or blocked must be notified of the decision and the reasons for it.

5.1.3. The service provider must have measures in place to prevent reported illegal or harmful content from being accessed again on the service.

5.1.4. The service provider must explain and document how reported incidents are processed and acted upon.

5.1.5. The service provider must provide contact points on the service for the police and Danish reporting and help services, such as Red Barnet (Save the Children), Børns Vilkår (Children's Welfare), and Center for Digital Pædagogik (Center for Digital Youth Care).

5.2. The service provider must generally make visible and report in an anonymized form which and how many complaints and breaches of guidelines the service provider has received as well as measures taken in this regard.

6. Behavioral design must not be used to retain children

6.1. The service provider must not use artificial intelligence and behavioral influencing mechanisms that unnecessarily stimulate children's behavior and maintain their use of the service, such as chat bots[5], continuous scrolling, streaks, auto-play, etc.

6.1.1. Recommendation systems that are used to prioritize and recommend content and information without the user acting on it must be disabled by default. Exceptions to this are recommendation systems in search functions that the user will actively use to find content or information. Recommendation systems must be age-appropriate, transparent, and the child/parent must be informed of the consequences of this in accordance with the principles in section 2.1.

6.1.2. The service provider must not recommend that children add or follow persons over 18 years of age and vice versa.

6.1.3. The service provider must also ensure that persons over the age of 18 can only send messages to persons under the age of 18 that the child has accepted.

6.1.4. Push notifications must be disabled by default. It must be possible to turn on push notifications individually and with a time limit. Upon activation, the service provider must inform about the consequences the change may have in relation to stimulating the child's behavior and use, cf. the principles in 2.1 and 3.1.1.

6.1.5. The service provider must make the total number of likes (or similar) invisible by default. The service provider must not have a dislike function on the service.

6.1.6. Unnecessary notifications about friends' and connections' activity and online status must be turned off by default. This includes, for example, friends' latest log-in, online status, set notifications, or anything else that indicates active use. If the child/parent wants one or more of the settings activated, the child must be able to turn them on individually, and the service provider must inform, cf. the principles in 2.1, about the consequences the change may have in relation to the stimulation of the child's behavior and use, cf. the principles in 3.1.1.

6.2. The service provider must make it easy to log out, to have data deleted at the user's request, and to delete their profile.

6.3. The service provider must support that content that has been retouched or manipulated is marked as such, e.g., by automatic tagging or by technically offering tagging and introducing mandatory tagging for users with many followers.

6.4. The service must by default activate a time limit for use, e.g., 60 minutes daily, and by default activate 'quiet-mode' from 22:00-06:00. If the child/parent wishes to disable these functions, they must be informed of the consequences in an age-appropriate and understandable manner, cf. the principles in 2.1 and 3.1.1.

[5] This refers to chatbots integrated into digital services covered by the guidelines. These are not stand-alone language models.

6.5. The service provider must offer safety and security enhancing parental controls and make it clear to the child whether parental controls are activated and what this means for the child.

7. It must be clear what the service monetizes and how

7.1 The service provider must ensure transparency about its business model and mechanisms used by the service.

7.1.1. The service provider must not create pressure on children, including the use of behavior-influencing mechanisms, cf. section 6, that encourages the spending of money or virtual resources.

7.2. The service must disable the ability to make purchases or donate money to/from other users or the service provider by default. If the child/parent wishes to enable these functions, they must be informed of the consequences in an age-appropriate and understandable manner, cf. the principles in 2.1 and 3.1.1. The functions must be adjustable with parental control, e.g., in the form of parental approval before each transaction, by setting limits on possible spending, and by automatic deletion of card details.

7.2.1. The service provider must display an overview of the child's monthly financial consumption and consumption per session on the child's profile. Regardless of whether the child uses virtual currency, items, or other resources in transactions, it must appear how many Danish kroner the use of resources corresponds to, both on the consumption overview on the profile and in the individual transaction.

8. The service providers must cooperate with authorities and researchers

8.1. Service providers must actively and on request cooperate with authorities.

8.1.1. For prevention purposes, the police must be able to act openly and visibly as an authority and interact with the users of the service.

8.1.2. The service must, in accordance with the applicable legislation, support police investigations in relation to illegal behavior and content.

8.2. The service provider must cooperate with independent researchers and research institutions and ensure they have access to its information and data for the purpose of social enlightenment. This can be further supported by an independent expert panel that can qualify the service's efforts with a focus on children and thereby contribute to increased transparency.

8.2.1 Digital service providers must provide independent researchers with insight into, among other things, the mechanisms, and interactions on the service.

8.2.2 Digital service providers must provide independent researchers with insight into children's use of the specific service and thus contribute to qualified protection measures.