European Commission

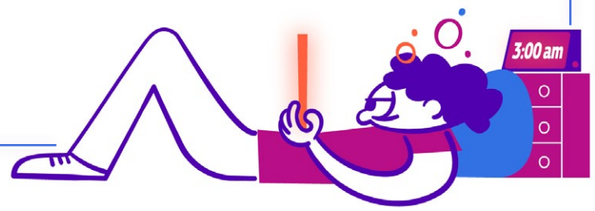
The Digital Services Act explained

What online platforms should do to keep kids and teens safe online

What is the Digital Services Act?

Online platforms are a big part of everyday life for children and teenagers, whether it's for meeting friends, watching videos, playing games or learning something new. But being online also comes with serious risks. Kids and teens might:

- *be cyberbullied;*
- *be contacted by strangers with bad intentions;*
- *see harmful or upsetting content that makes them feel uncomfortable, scared or disturbed;*
- *feel pressured to buy things;*
- *participate in dangerous challenges;*
- *find it hard to put the phone down or switch off the console.*



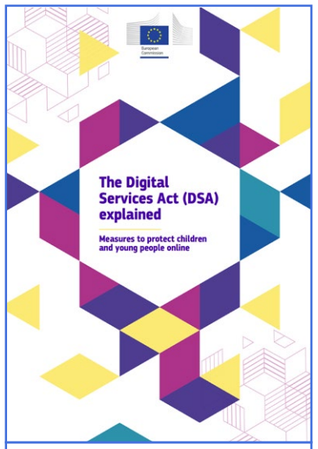
To help make the internet safer, in 2022 the European Union (EU) created the Digital Services Act (DSA). This law applies to online platforms (European or not) available in the EU. It aims to help keep all internet users – including kids and teens – safe from these and other risks, and protect fundamental rights online.

All online platforms must follow this law and help keep users safe in the EU.

How does the Digital Services Act keep kids and teens safe?

The DSA says that **online platforms must ensure a high level of privacy, safety and security for minors using their services**. This means that children and teenagers should feel protected and safe when they use apps, social media and games that are covered by the law. The largest platforms, which have more than 45 million users in the EU, like TikTok, Instagram and Snapchat, must also identify and assess other potential risks for children and teenagers who use their services.

In July 2025, the European Commission published guidelines on the protection of minors to help all platforms understand what they should do to keep kids and teens safe online. This booklet explains how the guidelines work.



Do you want to learn more about the DSA? Check out this booklet explaining the measures to protect kids and teens online.

What is inside?

Please note that this publication is intended for information purposes and does not constitute a legal document.

1. Who has to follow the guidelines on the protection of minors?

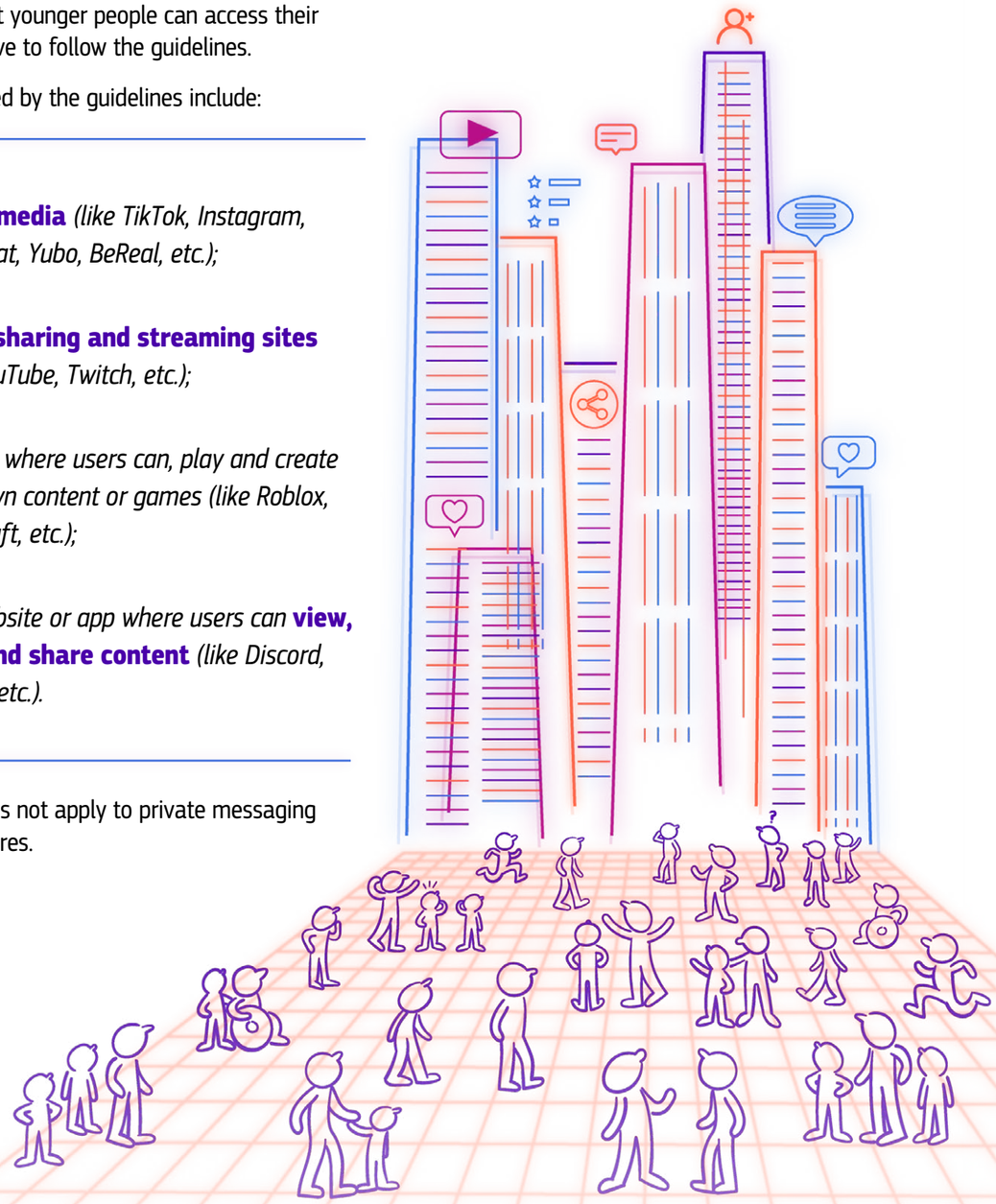
If a platform is used by kids and teens – or if it's likely they may access it – then the platform **must** follow the DSA rules and the guidelines on the protection of minors.

Websites made for grown-ups can't just say 'kids are not allowed' in their rules and ignore what's really happening. If they know that younger people can access their content, they have to follow the guidelines.

Platforms covered by the guidelines include:

- **social media** *(like TikTok, Instagram, Snapchat, Yubo, BeReal, etc.);*
- **video-sharing and streaming sites** *(like YouTube, Twitch, etc.);*
- **games** *where users can, play and create their own content or games (like Roblox, Minecraft, etc.);*
- *any website or app where users can* **view, post and share content** *(like Discord, Reddit, etc.).*

NB: The DSA does not apply to private messaging services or features.



2. What are the key principles?

The guidelines are built on three main ideas.

1. Children's rights come first

Platforms should respect children's rights and always act in the child's best interests. These rights include:

- *protection,*
- *non-discrimination,*
- *inclusion,*
- *privacy,*
- *access to information and education,*
- *freedom of expression,*
- *participation.*

This means designing, developing and operating platforms that are always *private, safe* and *secure*.

2. Safety by design

Platforms should not wait for problems to happen. They should build privacy, safety and security into their services from the start. Features should be appropriate for different ages and stages of children's development.

3. Understanding the needs of users

Platforms need to carefully consider how their services are used by children and teenagers, and what risks they might face, such as:

- *cyberbullying,*
- *harmful content,*
- *excessive use.*

Then, they must find solutions to reduce those risks.

3. Recommendations

Let's take a look at the recommendations that online platforms need to follow to protect kids and teens online.

a. Risk assessment: every platform comes with different risks

The guidelines recommend that platforms should **regularly check** whether their services pose **risks to kids and teens** and understand how and why. They need to find the right balance between:

- *letting kids and teens share their content, ideas and thoughts;*
- *giving them the chance to explore, play and learn new things online...*

... while keeping them safe!

Once risks are identified, platforms should respond with effective solutions – without limiting the important opportunities and benefits that children and teenagers can enjoy online.

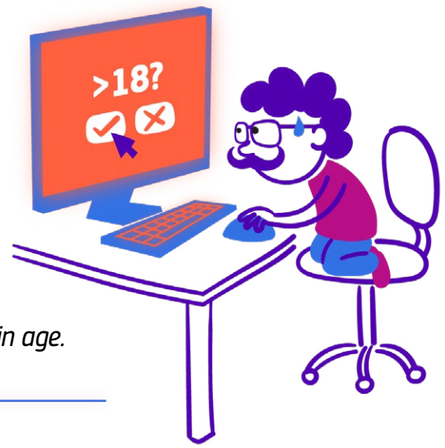
b. Age assurance: how platforms check your age

To make platforms safer – and to prevent kids and teens from using services that are not meant for them – it's important to know whether users are **old enough** to access certain content.

This is where **age assurance** comes in.

Age assurance means using tools to:

- *find out or estimate a user's age; or*
- *confirm whether someone is above or below a certain age.*

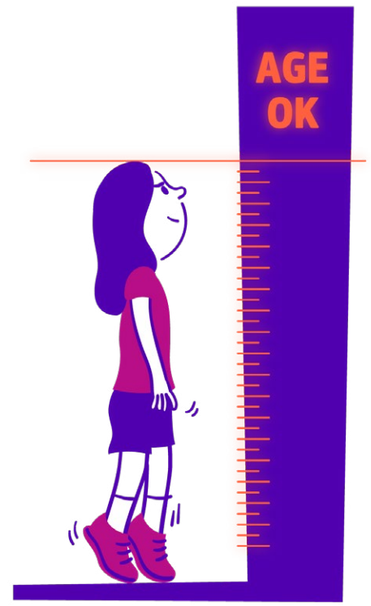


Did you know?

You have to be at least 13 years old to use TikTok, Snapchat, Instagram, BeReal and Steam!

Types of age assurance

There are three main ways platforms can check a user's age.



1. Self-declaration
You enter your date of birth, or click 'Yes, I'm over 13' or 'Yes, I'm over 18'. It's quick, but easy to cheat, so it's **neither effective nor reliable**.

2. Age estimation
Technology estimates your age based on things like:

- face scans,
- typing style,
- what you're interested in.

It's not perfect – it can't tell your exact age, and it might be **intrusive** to your privacy.

3. Age verification
This is the **most accurate** method. It checks your age using:

- official documents, like a passport,
- trusted digital IDs, like an ID issued by the government, or the EU Digital Identity Wallet.

This last method **protects your privacy** because users can prove their age without revealing any other personal data.

EU Digital Identity Wallet

What's the EU Digital Identity Wallet? It's a free app (coming in 2026) that helps people in Europe:

- keep important documents safe in one place;
- prove who they are, online and in real life.

It's like a digital backpack for your ID and important papers.

3. Recommendations

Online platforms should:

- *explain age checks in a way that's* **easy to understand** *for kids and teens;*
- *only ask about age when it's* **really needed** *to help keep users safe;*
- *use the* **simplest method** *that works well without asking for more information than needed;*
- *make sure all age assurance methods are* **accurate**, **fair**, *and* **hard to bypass;**
- *offer* **more than one option**, *so no one is left out;*
- *allow users to* **appeal** *if their age is not estimated correctly.*

What method should platforms use?

Low-risk services	Medium-risk services *e.g. certain social media platforms*	High-risk services *e.g. gambling, dating and adult content, or any content rated 18+*
Recommended method: Other safety measures may be enough	*Recommended method:* **Age estimation** or age verification	*Recommended method:* **Age verification**

Age assurance looks a bit complicated, doesn't it?
This guide to age assurance can help you understand!

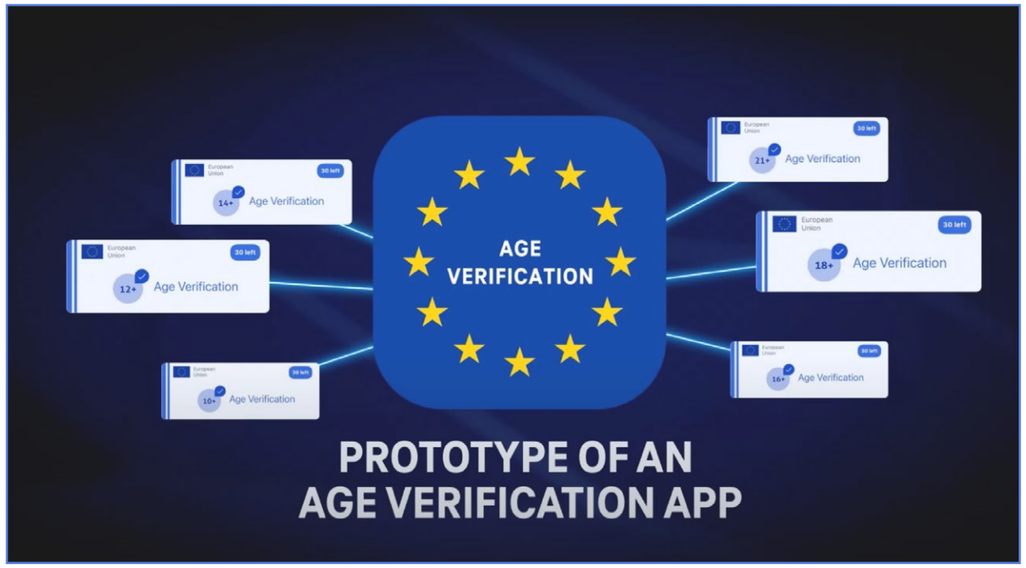
Can an app really verify your age?

Yes! The European Commission is working on a solution for you! In July 2025, it launched a **blueprint for an age-verification app.**

It's designed to:

- *be user-friendly;*
- *allow users to prove that they are 18 or over;*
- *avoid asking for any other personal details.*

This helps keep access to certain online content **safe and age appropriate**.



Are you curious about the EU's approach to age verification? Scan the QR code to learn more!

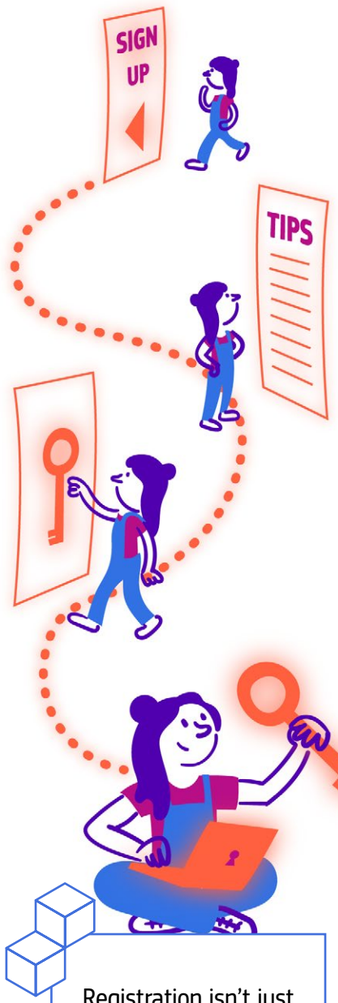
c. Registration: information and empowerment from the start

When a platform asks users to register, it's often a good opportunity to:

- *share important* **safety information**;
- *provide* **educational tips**;
- *ensure the user is* **old enough** *to access.*

To do this well, platforms need to:

- **clearly explain** *why registration is needed and what the benefits are*
- *keep the* **process simple and accessible**, *especially for kids and teens with additional needs or disabilities*
- *avoid encouraging users who are* **too young to sign up**
- *make it easy for children and teens to* **log out** *or* **delete their accounts** *at any time*
- *use registration to introduce and explain* **key safety features** *like:*
  - > privacy settings
  - > default protections
  - > reporting tools
- *help children and teens understand:*
  - > what **safety tools are available**
  - > how to **get help** if needed.



Registration isn't just about creating an account. It's a chance for the platform to make sure young users start off **safe**, **informed** and **in control**.

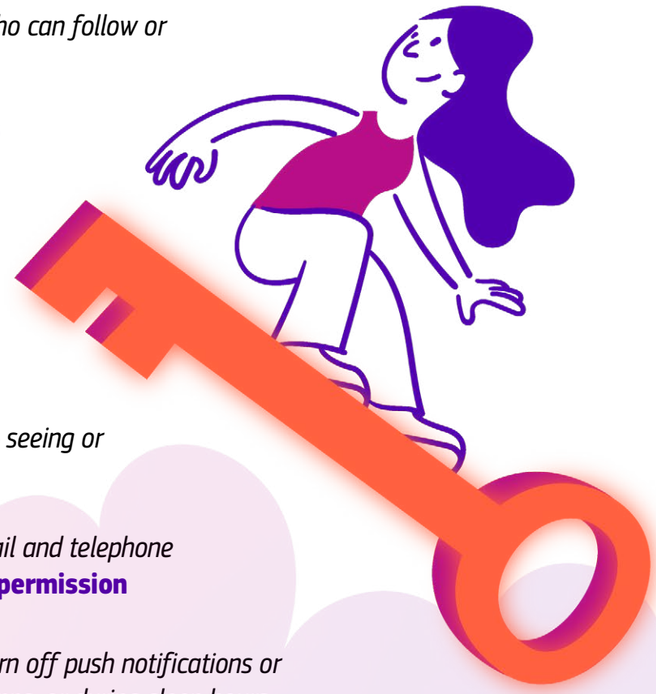
d. Account settings: privacy and safety you can control

Account settings can help children, teenagers and their parents or guardians manage their online presence – like how much personal information is visible to others, or how easy it is to be contacted.

Since most people don't change the default settings, platforms need to make sure these are **private, safe and secure from the start**.

Default settings should include:

- **Limiting contact:** *control who can follow or message the child or teen*
- **Turning off risky features** *by default, such as:*
  - > geolocation
  - > autoplay of videos
  - > microphone and camera
  - > contact syncing
  - > tracking.
- **Preventing strangers** *from seeing or downloading content*
- *Sharing contact info (like email and telephone number)* **only with explicit permission**
- **Managing notifications***: turn off push notifications or alerts from certain users or apps, or during sleep hours*
- **Reducing excessive use** *by turning off features like:*
  - > likes and reactions counters
  - > "...is typing" features
  - > read receipts.
- **Protecting mental health:** *turn off image filters that may negatively affect body image or self-esteem.*



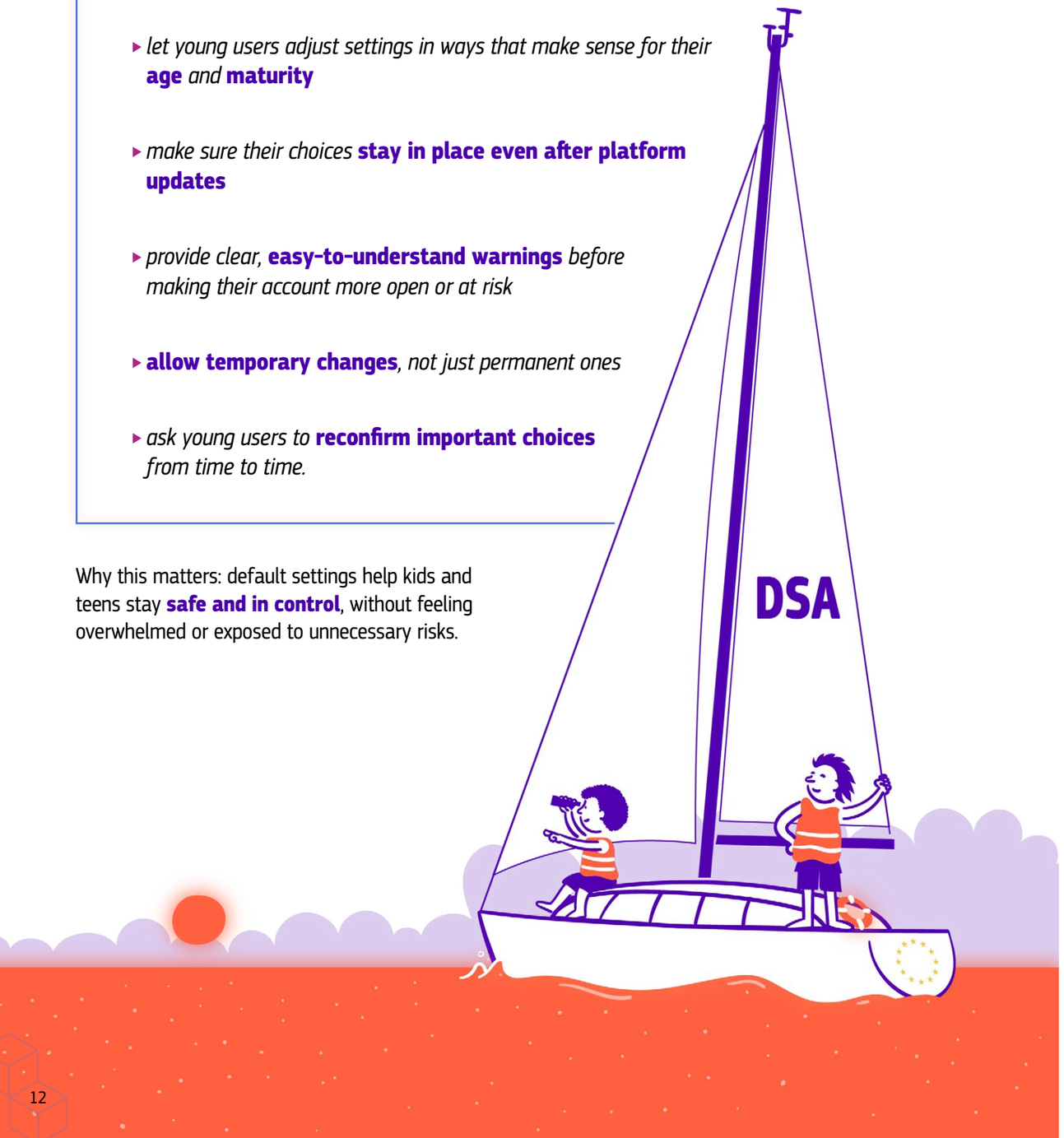
Giving kids and teens control – with guidance

Kids and teens should never be encouraged to lower their privacy, safety and security settings. But if they want to **customise their experience**, they should be able to do so in a way that's safe and age appropriate.

Platforms need to do:

- *let young users adjust settings in ways that make sense for their* **age** *and* **maturity**
- *make sure their choices* **stay in place even after platform updates**
- *provide clear,* **easy-to-understand warnings** *before making their account more open or at risk*
- **allow temporary changes**, *not just permanent ones*
- *ask young users to* **reconfirm important choices** *from time to time.*

Why this matters: default settings help kids and teens stay **safe and in control**, without feeling overwhelmed or exposed to unnecessary risks.



e. Interfaces: designing platforms to be easy and safe to use

An **interface** is how an online platform looks and works – what you see on your screen and how you interact with it. A well-designed interface can help kids and teens **stay safe, feel confident** and **enjoy their time online**.

To prevent excessive use and addictive behaviours, and make it easier to log off, platforms should avoid features like:

- *infinite scrolling – when the page has scrolled all the way to the bottom, it automatically refreshes with new content*
- *pull-to-refresh*
- *constant notifications*
- *video autoplay*
- *virtual daily rewards, streaks or points that require children to open the app or game every day.*

Platforms need to include:

- *tools that help kids and teens* **manage their time online**, *like friendly reminders to take breaks*
- *safety settings, and reporting and feedback tools that are* **easy to find, understand and use**
- **accessibility features** *for everyone, including children and teenagers with additional needs or disabilities*
- *clear* **warnings** *when children and teenagers are interacting with* **artificial intelligence** *(AI) features.*

f. Recommender systems and search features: helping kids stay in control

Do you ever wonder how your social media apps or your favourite TV shows' platforms always know what to show you next?
Recommender systems decide what kind of content or contact suggestions show up in users' feeds – including explore pages – based on what they've liked, watched, clicked on or decided to follow before.

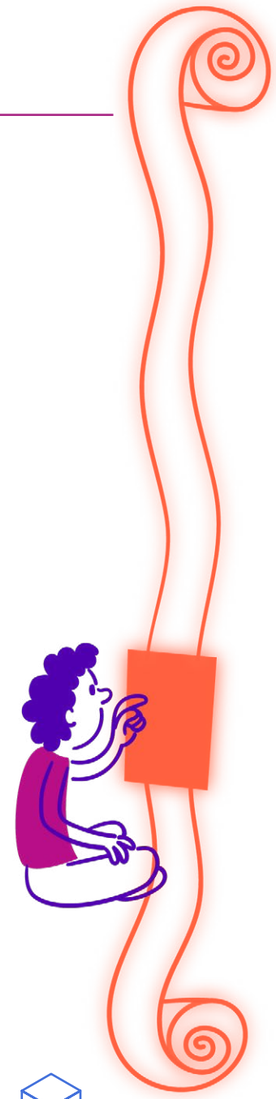
While this can be helpful, it can also lead kids and teens to see harmful or inappropriate images, videos, posts or commercial products.

Platforms should:

- *only show content that is* **age-appropriate**
- *limit how much* **data is collected and used** *to make recommendations*
- *prioritise active* **user choices and feedback**, *like:*
  - > 'Show me less/more of this'
  - > 'I don't want to see this'
  - > 'I am not interested in this'
- **avoid relying too much on passive feedback**, *like how long users watch or browse*
- *explain* **why something was recommended** *and how users can change it*
- *let users* **reset their feed** *completely and permanently*
- *make it easy to* **report unwanted content** *— and ensure feedback actually changes what is shown*
- *make all recommender system settings* **child-friendly and accessible**.

Search features should:

- *block unsafe words or hashtags*
- *help children and teens choose what interests them most.*



Recommender systems should empower kids and teens, not overwhelm them. Giving young users control over what they see helps build **safer, more positive online experiences.**

g. Commercial practices: helping kids and teens understand what's being promoted and sold

Children and teens – just like adults – may not always realise when something online is

- an advertisement ("ads")
- a hidden promotion
- a paid post by an influencer.

It can also be hard to spot how apps, games or websites try to convince us to spend more time or money. This can lead to unnecesary purchases or habits that are hard to break.

Platforms need to:

- *clearly and consistently label all advertising and sponsored content – including influencers'* **product placements**
- *regularly review how ads are labelled, and check with children and guardians that labels are* **clear and effective**
- *avoid advertising to children and teenagers products and services that could harm* **privacy**, **safety**, **and/or security**
- *be transparent about the costs and implications of:*
  - > **in-app purchases**
  - > **virtual currencies or tokens**
  - > other **transactions**.
- *Avoid pressure tactics like:*
  - > **countdown timers**
  - > **'buy now'** messages.
- *block access to any feature that resembles* **gambling**, *like* **loot boxes**
- *ensure "free" products and services don't include hidden purchases*
- *make sure advertising is* **age-appropriate**
- *adapt advertising algorithms so* **children are not exposed to ads too much or too often**.

Why this matters to you: These measures can help to protect kids and teens from being **tricked or pressured** into spending money when they don't want to.

What do these terms mean?

A **product placement** is when a brand or item is shown in a video or post as part of a paid promotion.

A **loot box** is a digital item that gives random rewards, often used in games.

An **in-app purchase** is something you buy inside an app, like extra features, more lives, new skins or virtual coins.

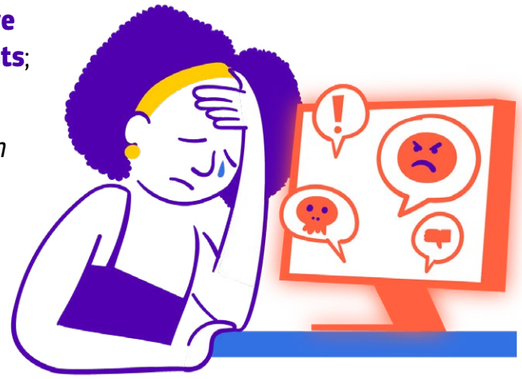
h. Moderation: keeping platforms safe and respectful

Moderation means **checking and removing content or users** that could harm kids' and teens' privacy, safety and security, including their overall physical and mental well-being.

It's an important tool to protect users and prevent serious risks such as bullying, exposure to harmful content, or grooming (when someone tries to be friends with a child or teen to trick them or make them feel uncomfortable).

Platforms should:

- *clearly define what is meant* **by harmful content and behaviours**;
- *use an efficient process to* **quickly remove harmful or illegal content and accounts**;
- *train moderators to spot threats to children and teenagers, such as* **grooming or dangerous challenges**;
- *remove illegal or harmful content* **without delay**;
- *use tools to* **prevent users from generating or sharing harmful AI content**;
- *regularly* **review and improve** *how moderation systems work.*



Good moderation helps create a space where kids and teens feel **safe, respected and supported**.

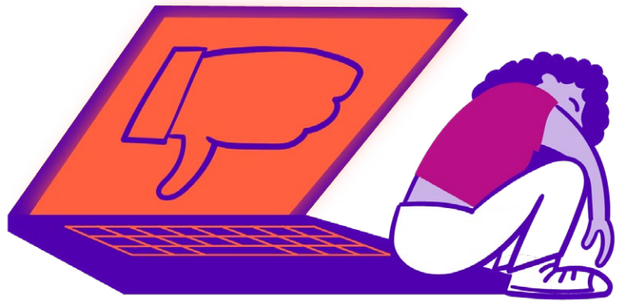
Moderation isn't just about removing content – it's about building a safer, more respectful online space for everyone.

i. Reporting: making it easy to speak up and get help

Sometimes things go wrong online. You might see something upsetting, be bullied or feel unsafe. That's why it's important that platforms make it **easy for everyone to report problems and get help**.

Platforms need to:

- *offer* **simple and clear ways** *for any user to* **report** *abuse, cyberbullying or harmful content (including persons with disabilities)*
- *allow users to* **block**, **mute or restrict** *comments and interactions with other users*
- *make sure that users aren't* **automatically added to groups** *– joining should only happen after accepting an invitation*
- *provide* **fast and helpful responses** *when users report a problem and feedback on what happened.*



Need help reporting upsetting content?

The network of Safer Internet Centres across Europe can help you!

Whatever you need to talk about, they offer support, practical help, guidance and someone to listen.

j. Tools for parents and guardians

Parents and guardians can help children and teens stay safe online. Platforms can offer tools that support this role, **without taking away the young person's rights or independence**.

If platforms choose parental control tools to complement their obligatory safety features, such tools should:

- *be based on* **communication and empowerment**, *not control;*
- **respect children's and teens' privacy**, *and notify them when a parent or guardian activates such tools;*
- *work across* **all devices and software versions**;
- *be compatible with* **existing parental tools**, *like the ones built into phones or apps.*

Tools for parents and guardians can help families build **trust and support** – but should never result in surveillance or take away a child's rights. They also shouldn't replace the platform's built-in safety features.

Need support as a parent or guardian? The Better Internet for Kids (BIK) Parent Corner offers tips to help your children build good digital habits and safely navigate the online world.

Each EU Member State has a **Digital Services Coordinator (DSC)** who works with the European Commission to supervise and monitor how platforms apply the DSA.

Scan the QR code to find out who the DSC is in your country

Each DSC can appoint organisations that are experts in identifying and flagging illegal and harmful content. They are called **trusted flaggers**, and when they raise concerns, platforms must act quickly! Think of them as referees who call out problems as soon as they spot them.

Scan the QR code to find out who the trusted flaggers are in your country.

5. What happens next?

The European Commission and Member States will continue to make sure platforms follow the DSA and keep children and young people safe online. Together they are:

- *checking if platforms follow the guidelines on the protection of minors under the DSA, and starting legal proceedings if they don't;*
- *testing and rolling out the* **EU age-verification app**;
- *developing an* **EU action plan against cyberbullying**;
- *analysing how* **social media use can impact mental health** *in children and teens.*

Digital age of majority
The age when you can start using online services on your own – without needing a parent's approval. It's usually 13 or 18, depending on the rules in your country and the type of service.

Your notes

Your notes

Your notes

Where can you get more information and help?

Full text of the DSA guidelines on the protection of minors online

Better Internet for Kids portal

Whether you're a child or teenager, parent, guardian or **educator**, you can contact the Safer Internet Centre in your country for help or information on any online issue.

Help is always available — by **phone**, **email**, or **online chat** – and it's **free**!

This family-friendly booklet explains the European Commission's protection of minors guidelines under the Digital Services Act in simple terms. It shows how online platforms should keep children and teens safe by putting their rights first, integrating privacy and safety in the design of the platform, checking age, making settings private, designing safe interfaces, moderating harmful content, making reporting easy, and supporting parents - so young people can enjoy the internet with confidence and support.

European Commission
Directorate-General for Communications Networks, Content and Technology
Printed by the Publications Office of the European Union in Luxembourg
Manuscript completed in October 2025

Download this booklet at:
https://link.europa.eu/cgyKch

PDF ISBN 978-92-68-31207-0 KK-01-25-130-EN-N doi:10.2759/7053090
Print ISBN 978-92-68-31208-7 KK-01-25-130-EN-C doi:10.2759/8280512

Publications Office of the European Union

DSA for YOUth