# Implementation Questionnaire

**2021**

# Introduction

---

**Notes/instructions on completing this template**
- Please complete all sections and all questions as far as possible
- Where a question or section is not applicable, please mark as N/A
- Where is overlap – or no change – to information previously submitted in company statement of commitments, please simply enter "refer to self-statement"
- URLs or screenshots (with links) are particularly useful in illustrating individual points
- Please add any additional information/data relevant to the submission at the end of the appropriate Principle

---

| **1. Name of the company on whose behalf this submission is made:** |
|---|
| Facebook Ireland |

| **2. Country or primary markets where products/services are offered (in EU) to which this submission applies. In which European markets does your company operate?** |
|---|
| All EU markets |

| **3. Product(s) or services included within the terms of this submission** |
|---|
| Facebook |

| **4. Nature of activity** |
|---|
| ☐ *Manufacturers of desktop and laptop computers, mobile phones, tablets, TV set top boxes and gaming consoles*<br>☐ *Network operators and connectivity providers*<br>☐ *Online content provider*<br>Ⅹ *Online service provider*<br>☐ *Other* (please specify): ...................................................................... |

| **5. Person(s) completing the report** |
|---|
| Name: David Miles<br><br>Position: Head of Safety - Europe, Middle East and Africa<br><br>Email: davemiles@fb.com |

# Principle 1 – Content

> **Commitments**
>
> Signatories should:
> - Indicate clearly where a service they offer may include content considered not to be appropriate for children and display prominently options which are available to control access to the content. This could include, where appropriate for the service, tools to manage access to certain content, advice to users or a recognised system of content labelling.
> - Display prominently and in an easily accessible location the Acceptable Use Policy, which should be written in easily-understandable language.
> - State clearly any relevant terms of service or community guidelines (i.e. how users are expected to behave and what is not acceptable) with which user generated content must comply.
> - Ensure that reporting options are in the relevant areas of the service.
> - Provide notice about the consequences for users if they post content which violates terms of service or community guidelines.
> - Continue work to provide innovative solutions able to support child safety protection tools and solutions.

**1. Do you provide a mechanism for consumers to _provide feedback, report an issue or file a complaint_ about the appropriateness of a piece of content?**

X *Yes*

☐ *No*

☐ *Not applicable* (please explain): ...........................................................

If yes, please provide details:

Facebook's mission is to give people the power to build communities and bring the world closer together. We're committed to building technologies that enable the best of what people can do together. Our products empower around 3 billion people around the world to share ideas, offer support and make a difference.

We take the issue of safety on our platform very seriously, especially that of our younger users. Our Terms of Service[1], Community Standards[2] and related policies aim to find the right balance between giving people a place to express themselves and promoting a safe and welcoming environment for everyone using our platform.

In order to enforce the Community Standards, we allow users to report content for our teams to review. If users see anything that makes them feel uncomfortable, feel it is inappropriate or violates our community standards, they can report it. Any piece of

---

[1]Available at: https://www.facebook.com/legal/terms

[2] Our Community Standards outline what is allowed and not allowed on the platform. They are available at: https://www.facebook.com/communitystandards/

content can be reported to our team.
Our specially trained reviewers provide 24/7 coverage and support over 50 languages. By combining technology and user reporting we are able to enforce our Community Standards at scale.

For information on the scale and effectiveness of our enforcement efforts, please see our latest Community Standards Enforcement Report[3] which covers enforcement activity across Facebook (and Instagram) for the previous quarter.

We are constantly innovating to develop ways to encourage user reporting, make it more accessible to more people, and to surface the option to report something to us at key moments where abuse may be occuring.

**2. Do you offer a means _for restricting / blocking access_ to potentially inappropriate content for users of your service or product?**

X *Yes*
☐ *No*
☐ *Not applicable* (please explain): ...........................................................

If yes, please provide details of mechanisms in place:

Facebook was developed to be safe by design for all users over the age of 13. In limited circumstances, this means a different user experience for different age ranges, but overall the platform was built to be safe for all users, regardless of age. These safeguards for all users include:

- **Privacy settings**. Users can choose their audience settings and who sees their content.

- **Safety tools to block, unfriend, mute, or restrict unwanted interactions**. The Services have easy-to-use in-app tools that allow users to "unfriend", "unfollow", or block accounts they do not want to interact with.

- **Controls to strengthen messaging privacy**. We provide a number of controls to protect users on our private messaging services.

- **In-app tools to report violating content**. Facebook has in-app reporting tools so that users can report accounts, post, comments, and direct messages that they feel are inappropriate and/or go against our Community Standards

- **Extensive support for potentially vulnerable users**. Facebook also provides anonymous reporting tools for content such as self-injury posts, so that we can connect the account reported to organisations that offer help, as well as anonymous reporting for live videos to report at-risk behaviour during a live broadcast, so the person reported receives a message offering help, support, and resources.

---

[3] Available at: https://transparency.fb.com/data/community-standards-enforcement

Implementation of the ICT Principles

- **Automated systems and technologies to prevent abuse**. Facebook utilises various technologies and automated systems to help reviewers take action on content that violates our Community Standards at scale.

- **Anti-Bullying tools and features**. We have developed a dedicated Bullying Prevention Hub[4] and continue to explore and develop safeguards in this important space.

- **Ads Restrictions, and Advertising and Branded Content Policies.** We apply numerous safeguards and restrictions around advertising:

  - We have strict advertising policies for advertising to all users, including minors, which impose high standards on paid advertising. Among other things, the Advertising Policies[5] and Branded Content Policies[6] strictly prohibit ads promoting the sale or use of certain types of products, such as tobacco and related products, drugs and drug-related products, and adult content.

  - As set out in the Data Policy[7], we do not sell users' information to anyone.

- **Time Spent tools for responsible social media use.** Since 2018, we have offered tools to help people manage their time on our services: an activity dashboard, daily reminder, and a way to limit notifications.

Specific provisions for users under the age of 18 include:

- **Ads Restrictions and Safeguards for under 18s.** We apply numerous safeguards and restrictions around advertising:

  - teen-specific safeguards which place restrictions on the personalisation of advertising to users under the digital age of consent.

  - further age-restrictions for ads for certain products or services, like alcohol, dating services, gambling, and weight loss products.

- **Educational resources for youth**. Facebook has a dedicated Youth Portal[8] designed to provide young users with general tips, helpful tricks, information about privacy and security, and everything else they need to have a positive experience on Facebook.

- **Educational resources for parents.** We also offer additional dedicated resources for parents on our services, including a dedicated Parents Portal.[9]

- **Public safety campaigns.** We operate a citizenship and wellbeing program called "Get Digital" which provides lessons and resources to help young people develop

---

[4] See: https://it-it.facebook.com/safety/bullying
[5] Advertising Policies: https://it-it.facebook.com/policies/ads/
[6] Branded Content Policies: https://it-it.facebook.com/policies/brandedcontent
[7] Data Policy: https://www.facebook.com/about/privacy
[8] Available at: https://www.facebook.com/safety/youth
[9] Available at: https://it-it.facebook.com/safety/parents

the competencies and skills they need to more safely navigate the internet.[10] These resources are designed to be used by young people,[11] as well as educators[12] and parents[13] both in the classroom and at home.

- **Adult-only features.** In addition to the advertising restrictions mentioned above, young users generally have a more limited experience on our services when it comes to the features they have access to, who they share and connect with, and the content they see. For example, as mentioned, Facebook Dating is available only to adults aged 18 and over who have a Facebook account in good standing,[14] only users who are 18 and over may offer or request mentorship in Facebook's mentorship groups,[15] and users must be 18 and over to buy and sell on Facebook Marketplace.[16]

**3. Do you provide any _information, educational resources or advice for users_ in any of the following areas?**
(tick as many as apply)

☐ _Content classification or labeling guidelines_
x _How to block or restrict access to content_
x _How to report or flag content as inappropriate_
x _Safe searching_
x _Information about your company's content policy in relation to children_
☐ _Not applicable_ (please explain): ............................................................

If yes, please provide details including the format of any material provided (video, text, tips, games, FAQs, etc.):

A wide range of safety educational resources, information and tips for users can be accessed on our Safety Centre[17] and our Help Centre[18].

Resources are available in multiple formats including:
- in-app and newsfeed education;
- short videos;
- comprehensive FAQs;
- user-friendly resources and guides available in more than 50 languages, many of them available to download in PDF format.

**4. Where is your company's _Acceptable Use Policy_ (AUP) located?**

---

[10] See: https://www.facebook.com/fbgetdigital/
[11] See: https://www.facebook.com/fbgetdigital/youth
[12] See: https://www.facebook.com/fbgetdigital/educators
[13] See: https://www.facebook.com/fbgetdigital/parents
[14] See: https://it-it.facebook.com/help/facebookdating
[15] See: https://it-it.facebook.com/help/380533659173752
[16] See: https://it-it.facebook.com/marketplace/learn-more/
[17] See: https://www.facebook.com/safety
[18] See: https://www.facebook.com/help

Implementation of the ICT Principles

Our Terms of Service[19] govern the relationship with our users or others who interact with our platform.

**5. Does the AUP or separate give clear guidelines with which <u>user generated content</u> must comply (including details about how users are expected to behave and what is not acceptable)?**

x *Yes*
☐ *No*
☐ *Not applicable* (please explain): ............................................................

If yes, please identify relevant policy:

In addition to our Terms of Service, we have developed a comprehensive set of Community Standards[20], which govern the content that is and is not allowed on Facebook. In developing these policies, we consult hundreds of civil society organisations and academics from around the world. When applying these policies, we seek to find a balance between safety and allowing users to have a voice.

The Community Standards cover a wide range of behaviour and content which is considered unacceptable and therefore not allowed on our platform. The Community Standards prohibit a wide range of content that may be considered harmful, or in some cases, inappropriate for younger users, including issues relating to: violence and criminal behaviour[21]; safety, such as suicide, self-injury, sexual exploitation, abuse and nudity, bullying and harassment, exploitation and privacy violations[22]; objectionable content[23]; integrity and authenticity[24]; and content-related requests and decisions[25]. The Community Standards specifically prohibit content that may incite violence or hatred on the grounds of discrimination. We define hate speech as content that attacks any individual based on 'protected characteristics', which includes race, ethnicity, national origin, disability, religious affiliation, caste, sexual orientation, sex, gender identity and serious disease. Although globally applied, the Community Standards do also cover certain issues that may also overlap with generalised and accepted categories of unlawful content including issues relating to: terrorism (in particular, violence and incitement, dangerous individuals and organisations, promoting or publicisng crime, coordinating harm and fraud and deception[26]); child nudity and sexual exploitation of children, human exploitation, sexual activity and sexual solicitation[27] [28]; and racism and xenophobia[29].

---

[19] https://www.facebook.com/legal/terms
[20] https://www.facebook.com/communitystandards/
[21] https://www.facebook.com/communitystandards/violence_criminal_behavior
[22] https://www.facebook.com/communitystandards/safety
[23] https://www.facebook.com/communitystandards/objectionable_content
[24] https://www.facebook.com/communitystandards/integrity_authenticity
[25] https://www.facebook.com/communitystandards/content_related_requests
[26] https://www.facebook.com/communitystandards/violence_criminal_behavior
[27] https://www.facebook.com/communitystandards/safety
[28] https://www.facebook.com/communitystandards/objectionable_content
[29] https://www.facebook.com/communitystandards/objectionable_content

Facebook also has specific policies in relation to advertising on the platform. Our Advertising Policies[30] provide guidance on what types of ad content are allowed on the platform. These policies complement our Community Standards, and set out additional rules governing ads on our platform.

**6. Do you provide notice about the _consequences for users_ if they post content which violates terms of service or community guidelines?**

☐ *Yes*

☐ *No*

☐ *Not applicable* (please explain): ...........................................................

If yes, please identify relevant policy:

People can check on the status of a report in their Support Inbox[31].

Users can appeal decisions for posts that were removed for bullying and harassment, nudity, sexual activity, hate speech or graphic violence and we are working to bring more violation types into the appeals remit.

In a small number of cases and for the most serious violations of our Community Standards e.g. the sharing or threat to share non-consensual intimate images and predatory behaviour towards children, users will be removed from the platform. In certain emergency circumstances, involving the immediate risk of harm, suicide prevention and the recovery of missing children, we may also bring such accounts to the attention of law enforcement.

---

[30] https://www.facebook.com/policies/ads/
[31] See here: https://www.facebook.com/support and here: https://www.facebook.com/help/338745752851127?helpref=about_content

Implementation of the ICT Principles

# Principle 2 – Parental Controls

---

**Commitments**

Signatories should assist parents to limit their children's exposure to potentially inappropriate content and contact.

- Manufacturers should optimise hardware design to provide products which simply and clearly help parents to set appropriate levels of control on devices.
- Network providers should provide necessary tools and settings across their services to enable parents to set appropriate levels of control.
- Service and content providers should make available the necessary tools and settings across their services to enable parents to set appropriate levels of control

---

**1. Please outline the availability of any _parental control tools and settings_ across your product or service that allows parents to set appropriate levels of control? Include relevant links/ screenshots where available:**

The Terms of Service[32] require people to be at least 13 years old to create an account on Facebook. Subject to the age of consent under the EU General Data Protection Regulation (GDPR) and in individual EU Member States, teenagers have full control over their account.

Facebook does not provide parental control mechanisms. Our philosophy is to empower parents to have conversations with their children about safe online use and to promote responsible online behaviour. In light of that, we have developed dedicated, expert informed resources through the Parents Portal[33] and the Bullying Prevention Hub[34] in the Safety Center[35].

**2. . If applicable, please describe the features offered by the _parental controls_? E.g. restricting web access, customization, monitoring, other restrictions.**

Facebook does not provide parental control mechanisms.

**3. In relation to parental controls, which of the following _educational and information resources_ do you offer?**
(tick as many as apply)

---

[32] https://www.facebook.com/legal/terms
[33] https://www.facebook.com/safety/parents
[34] https://www.facebook.com/safety/bullying
[35] https://www.facebook.com/safety

☐ *Company policy in relation to use of parental controls*
☐ *Guidance about how to use parental controls*
☐ *Educational or awareness-raising resources about the use of parental controls*
☐ *A promotional or marketing channel for the uptake of parental controls*
☐ *External links to educational material/resources about the use of parental control*

Facebook does not provide parental control mechanisms.

**4. Please outline any additional safety tools or solutions _not detailed above_ that relate to parental controls, including any planned implementation of new features or procedures?**

Facebook does not provide parental control mechanisms.

Implementation of the ICT Principles

# Principle 3 – Dealing with abuse/misuse

**Requirements**
Signatories should:
- Provide a clear and simple process whereby users can report content or behaviour which breaches the service's terms and conditions.
- Implement appropriate procedures for reviewing user reports about images, videos, text and other content or behaviour.
- Provide clear information to users on all available report and review procedures.
- Place and review regularly links to these reporting options in appropriate areas of the service (e.g. where users view user-generated content or interact with other users) and provide guidance on what to report.
- Place links to relevant child welfare organisations or specialist providers of advice (e.g. about anorexia or bullying) and other confidential helplines/support services in appropriate areas.
- Ensure that moderators who review user reports are properly trained to determine or escalate content or behaviour presented to them

**1. Please provide details of _company policy relating to abuse_ and misuse (involving images, videos, text and other content or behaviour) on your product or service.**

We recognize how important it is for Facebook to be a place where people feel empowered to communicate, and we take our role in keeping abuse off our service seriously. That's why we have developed a set of Community Standards[36] that outline what is and is not allowed on Facebook.  Our Standards apply around the world to all types of content including: images; videos; text; and other content or behaviour and a broad range of harms and abuses such as: direct threats; nudity; graphic content; bullying and harassment; sexual exploitation; fraud; spam; intellectual property infringements; and more.

We encourage our users to report content to us that they believe violates our Community Standards, using the dedicated tools on the platform. Reports are prioritized based on potential real-world harm and triaged to ensure the most appropriate team reviews them. Our specially trained reviewers provide 24/7 coverage and support over 50 languages. By combining technology and user reporting we are able to enforce our Community Standards at scale.

By combining technology and user reporting we are able to enforce our Community Standards at scale. For more information on the scale and effectiveness of our enforcement efforts, please see our latest Community Standards Enforcement Report[37]

---

[36] https://www.facebook.com/communitystandards
[37] https://about.fb.com/news/2021/08/community-standards-enforcement-report-q2-2021/

which covers enforcement activity across Facebook (and Instagram) for the previous quarter.

**2. Please describe the _process or mechanism_ available for users to report abuse/misuse (involving images, videos, text and other content or behaviour) on your product or service).**

Every piece of content published on Facebook can be reported to our support teams for review, via the multiple reporting links available on the site. These reporting links are available across all device types (tablet, desktop, and mobile phones).

To report a piece of content on Facebook, users can click on the three dots that appear next to the content itself. There you'll find an option to "Find support or report" the piece of content. In order to report a comment, users can long press on the comment, and then click on "Find support or report comment"

The Facebook Help Centre[38] offers additional ways for people to report content to us.

All reports are anonymous, and the user reported isn't notified.

Once a report is made, we review it and remove anything that goes against our Community Standards. Our specially trained reviewers provide 24/7 coverage and support over 50 languages.  We also keep users updated on the status of their reports in the Facebook Support Inbox.

**3. _Where_ is the reporting button/ mechanism located?**
(tick any that apply)

x _On each page of the website/service_
x _Close to the point where such content might be reported_
x _In a separate location such as a safety page_
☐ _In a browser extension_
☐ _In a separate app for a connected device_
☐ _Other_ (please specify): ........................................................

**4. _Who_ may use such a reporting mechanism?**
(tick any that apply)

x _Only registered user/profile in which content is located_
x _All registered users of the product/service?_
☐ _Everyone including non-users, e.g. parents/teachers who are not registered for the service_
☐ _Other_ (please explain):  .......................................................

Any user can report and every piece of content can be reported to us.

---

[38] https://www.facebook.com/help

Implementation of the ICT Principles

| **5. Which of the following _kinds of content_ can users report?** |
|---|
| Every piece of content published on our platform can be reported to our support teams for review. |

| **6. Which of the following information do you provide to users?**<br>(tick any that apply) |
|---|
| x _Advice about what to report_<br>x _Advice about how to make a report_<br>x _Pre-defined categories for making a report_<br>x _How reports are typically handled_<br>x _Feedback to users_<br>x _Other website/external agency for reporting abuse/ misuse content?_<br>☐ _Other_ (please specify): ............................................. |

| **7. Please provide details of any _other means_, in addition to a reporting button/icon, to report content or behavior which breaches your service's terms and conditions** |
|---|
| Apart from the reporting features explained above, Facebook provides a dedicated Trusted Partners channel for key/selected international and non-governmental organisations to submit high quality reports on content that violates our policies and/or local law. |

| **8. Please outline briefly any other procedures or programmes offered by your service _not detailed above_ that relate to abuse /misuse,** |
|---|
| / |

# Principle 4 – Child Sexual abuse content or illegal contact

**Requirements**

Signatories should:

- Co-operate with law enforcement authorities, as provided for in local law, regarding child sexual abuse content or unlawful contact.
- Facilitate the notification of suspected child sexual abuse content to the appropriate law enforcement channels, in accordance with existing laws and data protection rules.
- Ensure the prompt removal of illegal child sexual abuse content (once it has been confirmed as illegal by the relevant public authority) in liaison with national law enforcement.
- Provide relevant additional information and/or links to users so they can make a report or obtain information about appropriate agencies or organisations that users can contact about making a report or obtaining expert advice, at national and EU level (e.g. law enforcement agencies, national INHOPE hotlines and emergency services).

---

**1. Which of the following mechanisms are provided on your product or service to _facilitate_ _the notification or reporting_ of suspected child abuse content?**
(tick any that apply)

☐ *Company-own hotline reporting button or telephone number*
x  *Link or button for external national or regional INHOPE hotline*
x  *Emergency services*
x  *Law enforcement agency*
x  *Other external agency* (please specify): ...........................................................

Our comprehensive approach to child safety across our family of apps includes: robust policies prohibiting child exploitation; cutting-edge technology to prevent, detect, remove and report violating content; and victim resources and support.

More than 35,000 people work across safety and security worldwide at Facebook. Our specially trained teams with backgrounds in law enforcement, online safety, analytics, and forensic investigations review potentially violating content and report apparent child sexual exploitation to the National Center for Missing and Exploited Children (NCMEC). In turn, NCMEC works with law enforcement agencies around the world to find and help victims.

Technology is our business, and we use a range of industry-leading tools and technologies to fight child sexual exploitation. We use these along all three prongs of our approach to child protection (i.e. prevention, detection, and response) and in ways tailored to public spaces like Pages, Groups, and Profiles, as well as, as appropriate and where permitted by applicable law, to our private messaging services.

Among the detection technologies we use - as far as legally permitted - are photo and video-matching technologies that help us detect, remove, and report the sharing of images and videos that exploit children. These technologies create a unique digital signature of an image (known as a "hash") which is then compared against a database containing signatures (hashes) of previously identified illegal images to find copies of the same image. We use these technologies across our public surfaces, as well as on non-encrypted information available to us on our private messaging services, including profile pictures and user reports. We also run these technologies on links from other internet sites shared on our apps and their associated content to detect known child exploitation housed elsewhere on the internet. This helps keep our services safer, and also helps keep the broader internet safer.

In addition to photo- and video-matching technology that detects known images, we use artificial intelligence and machine learning to proactively detect child nudity and previously unknown and new child-exploitative content[39], as far as such proactive detection is permitted by law. For example, we use this and other technology on the public and non-encrypted surfaces in our apps to more quickly detect such content and report it to NCMEC.

---

[39] https://about.fb.com/news/2018/10/fighting-child-exploitation/

Moreover, in order to prevent possible inappropriate interactions with children (IIC) from taking place between adults and minors on our private messaging services, we have developed techniques which rely, in part, on the use of traffic data. For example, where permitted by law, we use a combination of information from our public platforms and critical traffic data, to understand if an adult is attempting to contact children. We'll then take a decision on whether this means we should restrict all or some of the functions this user has available to them in order to prevent the likelihood of harm.

We also encourage our users to report content to us that they believe violates our policies using the dedicated tools on the services.
Following consultations with child safety experts and organizations, we have made it easier to report content for violating our child exploitation policies. To do this, we added the option to choose *"involves a child"* under the "Nudity & Sexual Activity" category of reporting. These reports are prioritized for review.
We are constantly innovating to develop ways to encourage user reporting, make it more accessible to more people, and to surface the option to report something to us at key moments where abuse may be occuring.

We are deeply committed to combating child exploitation and abuse across our platform and around the world and continuously seek out opportunities to contribute and advance multi-stakeholder efforts to eradicate its presence online.

Child protection requires a global and comprehensive response from industry, law enforcement, government, civil society and families, which is why Facebook is committed to working with child safety stakeholders worldwide to build and support the child safety ecosystem. Because online child exploitation is a global internet problem, it demands a global internet solution.

Several organizations and initiatives bring together industry and other players in the fight against child sexual abuse such as the Technology Coalition, an association dedicated solely to eradicating the sexual exploitation of children online, and international multi-stakeholder organizations like the WePROTECT Global Alliance to end child exploitation[40].

Last year, Facebook, Google, Microsoft and 15 other technology companies came together to announce *Project Protect[41]: A plan to combat online child sexual abuse* – a renewed commitment and investment expanding the Technology Coalition's scope and impact to protect children online and guide its work for the next 15 years.

Additionally, we work closely with our Safety Advisory Board[42] of leading online safety non-profits, as well as over 400 safety experts and NGOs from around the world, including specialists in the area of child sexual exploitation and victim support. We are committed

---

[40] https://www.weprotect.org/
[41] https://www.technologycoalition.org/2020/05/28/a-plan-to-combat-online-child-sexual-abuse/
[42] https://www.facebook.com/help/222332597793306

Implementation of the ICT Principles

to educating people on how to stay safe online and work with industry, NGOs, and other stakeholders to ensure people have the resources they need to stay safe.

**2. Please outline briefly the procedures to be followed if illegal content were to be discovered on your service.**

While prevention is our primary focus, reporting abusive and exploitative content to the relevant, competent authorities, which provides evidence for investigations and potential prosecution, is an important part of the holistic approach to tackling child sexual abuse.

As part of our commitment to fighting child sexual abuse, Facebook has specially trained teams which review content and report apparent child sexual exploitation to NCMEC[43] in compliance with applicable law. This is known as a CyberTipline report, with the CyberTipline providing the means for individuals and electronic service providers to lawfully report internet-related and other instances of child sexual exploitation. Following receipt of a CyberTipline report, NCMEC will determine a potential geographic location, and make the CyberTipline report available to a law enforcement agency in that particular country and location for review and potential investigation. NCMEC's deconfliction service ensures that reports are forwarded by NCMEC to the most appropriate law enforcement agency and, as such, avoids duplication of law enforcement resources. NCMEC also serves as an information clearinghouse and international resource center on issues related to victims, missing and exploited children.

NCMEC is a private, non-profit corporation whose mission is to help find missing children, reduce child sexual exploitation, and prevent child victimisation. It works with families, victims, private industry, law enforcement, and the public to assist with preventing child abductions, recovering missing children, and providing services to deter and combat child sexual exploitation.

In August 2019, NCMEC launched an updated Case Management Tool, funded by Facebook and developed with guidance and direction of our engineers. The tool is now available to law enforcement around the world -- making it easier for law enforcement to access reports in order to prioritise and respond to reports of child sexual exploitation. Over the years, NCMEC has developed relationships with law enforcement authorities globally and has established secure VPNs to support international cooperation.

We have developed a streamlined online process through which we respond to all legal requests from law enforcement and have a team dedicated to building strong relationships with the likes of NCMEC, ICMEC, CEOP, Interpol, Europol, the FBI, and numerous other local, federal and international law enforcement organizations and departments to ensure they have the information and training needed to make the best use of this process.

**3. Do you provide links to any of the following to enable users gain _additional information_ in relation to child sexual abuse content or illegal contact?**
(tick any that apply)

---

[43] http://www.missingkids.com/home

Implementation of the ICT Principles

x *Links to relevant child welfare organizations/specialist providers of advice*
x *Other confidential helplines/support services*
x *Law enforcement agencies*
x *INHOPE*
☐ *Other* (please specify): ……………..

Links to relevant child welfare organizations, confidential helplines and hotlines can be found throughout our Safety Centre[44] and Help Centre[45]. We are continuously working to improve all of these resources and make them as user friendly as possible, in multiple languages.

Information on the amount of child nudity or sexual exploitation content we remove is regularly updated in our Community Standards Enforcement Report[46].

**4. Please outline briefly any additional procedure in place within your company _not detailed above_ to ensure that you comply with local and/ or international laws with regard to child sexual abuse and other illegal content?**

/

---

[44] www.facebook.com/safety
[45] www.facebook.com/help
[46] https://about.fb.com/news/2021/08/community-standards-enforcement-report-q2-2021/

Implementation of the ICT Principles

# Principle 5 – Privacy and Control

---

**Requirements**

Signatories should:

- Manage privacy settings appropriate for children and young people in ways that ensure they are as safe as is reasonably possible.
- Offer a range of privacy setting options that encourage parents, children and young people to make informed decisions about their use of the service and the information they post and share with others online. These options should be easy to understand, prominently placed, user friendly and accessible.
- Take steps, where appropriate and in accordance with legal obligations, to raise user awareness of different privacy controls enabled by services or devices and enable users to use these as appropriate.
- Make reasonable efforts to raise awareness among all parties, service, content, technology and application providers, including public bodies, of industry good practice in relation to the protection of children and young people online

---

**1. Please provide details of your company's published _privacy policy_ in relation to access, collection, sharing and further use of data from minors under the age of 18 when utilizing your product or service?**

This information is contained in our Data Policy[47] which describes the information we process to support Facebook and other products and features we offer.

**2. Are _distinct privacy settings_ deployed to prevent access to information for users under the age of 18?**

---

[47] https://www.facebook.com/about/privacy

Implementation of the ICT Principles

x *Yes*
☐ *No*
☐ *Not applicable (please explain)*: .....................................................

If yes, please briefly outline available age-appropriate privacy settings (Provide details including relevant links/ screenshots on your website)

We believe it is important to strike the right balance of giving young people all the things they love about our services while also keeping them safe. We have designed our services to be safe for all users, regardless of age, by integrating a comprehensive suite of safeguards applicable to its services. Where necessary and appropriate, Facebook has implemented further safeguards for young people, striking a balance between protecting young people and facilitating their connection and development in the digital environment.

We have implemented enhanced privacy and safety features to protect young people who use our services, for example:

- Stricter default privacy settings for teenagers and additional behind-the-scenes protection;
- We've designed many of our features to remind them of who they're sharing with and to limit interactions with strangers;
- Messages sent to minors from unconnected adults (who are not friends or friends of the minor's friends) are filtered out of the minor's inbox;
- We take steps to remind minors that they should only accept friend requests from people they know;
- New minor users are automatically defaulted to share with 'friends' only and their default audience options for posts do not include "public." If a minor wants to share publicly, the first time they want to do so they must go to their settings to enable the option and we remind them about the meaning of posting publicly;
- The tool for controlling which posts other people can tag you in is switched on by default for children;
- Location sharing is turned off for minors by default. When a teen turns on location sharing, we include a consistent indicator as a reminder that they're sharing their location;
- Children's profiles cannot be found on search engines off Facebook because we prohibit them from being indexed;
- We protect their sensitive information such as contact info, school or birthday appearing in search to a public audience, including unconnected adults;
- Advertisers are not allowed to show ads to minors that "promote products, services, or content that are inappropriate, illegal, or unsafe, or that exploit, mislead, or exert undue pressure on the age groups targeted." This would include, for example, ads for alcohol.

As the way we operate online continues to evolve, we are ensuring that our measures are reviewed and updated periodically. In that light, we have recently announced several new

Implementation of the ICT Principles

measures that will give young people a safer, more private experience on our services and build upon the current measures that we have in place, for example:

• Making it harder for potentially suspicious accounts to find young people

Encouraging young people to have private accounts is a big step in the right direction when it comes to stopping unwanted contact from adults. But we're going even further to make young people's accounts difficult to find for certain adults.

We've developed new technology that will allow us to find accounts that have shown potentially suspicious behaviour and stop those accounts from interacting with young people's accounts. By "potentially suspicious behaviour", we mean accounts belonging to adults that may have recently been blocked or reported by a young person for example.

Using this technology, we won't show young people's accounts in Explore, Reels or 'Accounts Suggested For You' to these adults. If they find young people's accounts by searching for their usernames, they won't be able to follow them. They also won't be able to see comments from young people on other people's posts, nor will they be able to leave comments on young people's posts. We'll continue to look for additional places where we can apply this technology.

• Limiting the options advertisers have to reach young people with ads

We're also making changes to how advertisers can reach young people. Starting in a few weeks, we'll only allow advertisers to target ads to people under 18 (or older in certain countries) based on their age, gender and location. This means that previously available targeting options, like those based on interests or on their activity on other apps and websites, will no longer be available to advertisers. These changes will be global. Allowing targeting of advertisements using these minimal factors enables us to ensure that young people receive age-appropriate and relevant ads. Furthermore, it allows us to enforce the various policies that are in place to protect the interests of children, including our Advertising Policies.

When young people turn 18, we'll notify them about targeting options that advertisers can now use to reach them and the tools we provide to them to control their ad experience. We believe in showing people relevant ads so they can discover and purchase products that are interesting to them. In order to show people the most relevant ads, advertisers choose the types of people they want to see their ads. That could include choosing to show their ads to people with certain interests (like basketball) or based on information that they - or other partners - share with us about their activity on their website and apps. That's information like whether someone put a certain pair of shoes in their shopping cart or browsed for a new summer barbeque. We already give people ways to tell us that they would rather not see ads based on their interests or on their activities on other websites and apps, such as through controls within our ad settings. But we've heard from youth advocates that young people may not be well equipped to make these decisions. We agree with them, which is why we're taking a more precautionary approach in how advertisers can reach young people with ads.

• Hiding likes

Recently we announced that our users have the option to hide their public like counts, so they can decide what information is useful and beneficial for them to see, and what isn't

• Addressing age assurance

In addition to the above changes, we are continuing to invest in finding the right age assurance solutions. We need to keep people who are too young off of our platform, and we want to make sure that those who are old enough to use the services receive the appropriate experience for their age. For example, users must be 18 years old and over to access Facebook Dating, and Facebook uses signals and models in addition to the user's stated age to help prevent under 18s from accessing this feature.

In our latest blog "How Do We Know Someone is Old Enough to Use Our Apps"[48], we have shared how we are tackling this issue from multiple angles - things like using AI to detect age and working with industry partners and experts to define industry best practices and forming new technical standards. This is complex territory, with competing interests and considerations. We're committed to working with experts and the broader industry to give young people a compelling and safe experience on our services.

**Please identify default settings for each _age category_ of under 18s, as relevant:**

We have one age category for teens, which is 13-17 years old.

**Please identify any steps you have taken to ensure that these settings are _easy to understand, prominently placed, user friendly and accessible_.**

The above settings apply to minors by default.

**3. Where are users able to view and change or update their privacy status? tick any that apply)**

x *On each page of the website/service*
x *At each point where content may be posted*
x *In separate location such as a settings/safety/privacy page*
☐ *In a browser extension*
☐ *In a separate app for a connected device*
☐ *Other (please specify):* ......................................................

Tools such as the Privacy Checkup, 'View As' tool, and Blocking have been created to give people the power to control their experience on Facebook, understand their privacy settings and manage human interactions online as efficiently as possible.

---

[48] https://about.fb.com/news/2021/07/age-verification/

Implementation of the ICT Principles

Every time you share something on Facebook, you choose exactly who can see it – public, friends, a customized list of specific friends, or even just you. With every post you can select your audience, therefore people have one-click control over the visibility of every single status update, comment, note, photo or video that they choose to post on Facebook. And in case you change your mind or make a mistake, you can change the audience selected at any time after a post is made.

In addition to giving people tools to control the audience, you can block anyone you don't want to interact with for any reason whatsoever. People choose who they want to be friends with and they can ignore anyone, by unfollowing them. If someone blocks someone else on Facebook, the blocked person is not told, and neither person can see each other, interact or communicate. Another option available is to unfriend someone, and the person will not be notified and you will no longer appear on that person's friends list.

**4. Which of the following _information, resources or help features_ (if any) are provided to encourage users to make informed decisions about their privacy or the information they share?**

☐ *Tips/advice to users at the point of setting privacy options*
☐ *FAQs*
☐ *Help or educational resources in a separate location of service*
☐ *Links to any external NGO agencies offering education or awareness-raising related to privacy*
☐ *Links to governmental or EC agencies (Office of Data Protection Commissioner, ENISA etc.) in relation to privacy and data protection*
☐ *Other (please specify):* .......................................................

We provide the following resources to our users:
- Privacy Basics: Our Privacy Basics[49] helps people manage their information on Facebook through a series of interactive modules. The modules are based on the top questions people ask in the Help Centre.

- Privacy Checkup: Privacy Checkup[50] walks people through a few quick steps to help make sure they're sharing information with the people they want.

- Security Checkup[51]: We think everyone should understand how to keep their Facebook account secure. Our Security checkup aims to give people a quick overview of their security settings and suggest some additional features.

- Youth Portal: We recognise our responsibility to reach and communicate with young people differently.  Our Youth Portal[52] in the Safety Center has a dedicated section on Facebook Basics, where young people can learn more about Facebook, security, safety and privacy.

---

[49] https://www.facebook.com/about/basics/
[50] https://www.facebook.com/privacy/checkup
[51] https://www.facebook.com/security/checkup
[52] https://www.facebook.com/safety/youth/facebook-basics

Implementation of the ICT Principles

- Privacy Education: We also include privacy education in-product, so people have relevant information, at the time they need it, to make meaningful choices about how to share their information on Facebook. For example, we remind people who have been posting privately for some time that they are, in fact, posting publicly— and to make sure they're sharing with their intended audience.

- Get Digital: Get Digital[53] includes research-based lessons and resources that help young people develop the skills they need to become empowered digital citizens. Get Digital provides young people, educators, parents and care-givers lesson plans and activities organized around five pillars -- Foundations, Wellness, Engagement, Empowerment and Opportunities-- to help build the core competencies and skills young people need to navigate the digital world in safe ways.

- We also feature a privacy dedicated section in the Facebook Help Centre[54].

**5. Please outline briefly any additional policies or activities (existing or proposed), _not detailed above_, to ensure that personal information is protected, using reasonable safeguards appropriate to the sensitivity of the information.**

/

---

[53] https://www.facebook.com/fbgetdigital/
[54] https://www.facebook.com/help/193677450678703

Implementation of the ICT Principles

# Principle 6 – Education and Awareness

**Requirements**

Signatories should:

- Educate children and young people and give them up to date information to manage their access and settings in relation to content, services and applications, adding support where possible to existing initiatives and partnerships.
- Provide advice about features of the service or functionality that are available to allow parents to improve the protection of children, such as tools to prevent access to certain types of content or service.
- Provide links to other sources of relevant, independent and authoritative advice for parents and carers, teachers, and for children.
- Provide access to information that will help educate parents, carers, teachers and children about media literacy and ethical digital citizenship, and help them think critically about the content consumed and created on the internet.
- Encourage parents and teachers to use this information and talk to their children/pupils about the issues arising from the use of online services, including such topics as bullying, grooming and, where relevant, cost management

| **1. Does your company provide its own _educational resources_ aimed at any of the following groups?** |
|---|
| ☐  Younger children, i.e. under 13s |
| x  Teenagers <18s |
| x  Parents and carers |
| x  Teachers and other adults |
| ☐  Others (please specify): …………………………………………… |

| **2. Which of the following _topics_ are included within your own company educational materials?** <br> **(tick any that apply)** |
|---|
| x  Online safe behaviour |
| x  Privacy issues |
| x  Cyberbullying |
| x  Download and copyright issues |
| ☐  Safe use of mobile phones |
| x  Contact with strangers |
| ☐  Other topics (please specify) ………………………………………… |

| **3. With reference to any educational material you provide, _which of the following methods do you use_? (tick any as apply)** |
|---|

☐ Documentation provided with product/contract on purchase/first registration

☐ A required presentation by salesperson completing sale

☐ Displays/leaflets positioned prominently in stores

x Notification by email / on-screen statement / other means when product or contract is purchased or first registered

x Prominent notifications, resources or pop ups on website

x Helpdesk (telephone or online)

☐ Other (please specify): ...............................................

A wide range of safety educational resources can be accessed on our Safety Centre[55] and our Help Centre[56] .

**4. Please provide details of any links to other _external organisations_, or relevant, independent and authoritative advice for parents/carers, teachers, and for children?**

We work closely with our Safety Advisory Board[57] of leading online safety non-profits, as well as over 400 safety experts and NGOs from around the world, including specialists in the area of child sexual exploitation and victim support.

We list various global and European online safety organisations and resources[58] on the resources section of our Safety Centre.

**5. Please provide details of any campaigns, or active involvement in _industry partnerships_ on specific topics to raise public awareness of digital safety for children and young people?**

Facebook is part of several organizations and initiatives that bring together industry and other players in the fight against child sexual abuse such as the Technology Coalition[59], an association dedicated solely to eradicating the sexual exploitation of children online, and international multi-stakeholder organizations like the WePROTECT Global Alliance to end child exploitation[60].

Last year, Facebook, Google, Microsoft and 15 other technology companies came together to announce _Project Protect[61]: A plan to combat online child sexual abuse_ – a renewed commitment and investment expanding the Technology Coalition's scope and impact to protect children online and guide its work for the next 15 years.

**6. Please provide details of any partnerships with _NGO, civil society or other educational agencies_ or campaigns to raise public awareness of digital safety for children and young people.**

---

[55] https://www.facebook.com/safety

[56] https://www.facebook.com/help

[57] https://www.facebook.com/help/222332597793306

[58] https://www.facebook.com/safety/resources

[59] https://www.technologycoalition.org/

[60] https://www.weprotect.org/

[61] https://www.technologycoalition.org/2020/05/28/a-plan-to-combat-online-child-sexual-abuse/

We work closely with our Safety Advisory Board[62] of leading online safety non-profits, as well as over 400 safety experts and NGOs from around the world, including specialists in the area of child sexual exploitation and victim support.

We list various global and European online safety organisations and resources[63] on the resources section of our Safety Centre.

Below you can find a few examples, among many, of current campaigns and initiatives we are supporting to raise public awareness of digital safety for children and young people:

- Ireland - FUSE[64], in partnership with the National Anti-Bullying Research and Resource Centre in Dublin City University (DCU) , is an anti-bullying and online safety programme focused on teacher training, pupil participation and online parental resources. The aim of FUSE is to connect the whole school community as one to empower them to tackle bullying and online safety together. FUSE is grounded in Irish and international best practice research, consisting of a series of workshops and projects aimed at both primary and post-primary schools.

- UK - The Diana Award Anti-Bullying Ambassador Programme[65], in partnership with The Diana Award and Childnet International, offers every secondary (13+) school in the UK a Digital Safety Ambassador. A pupil in every school is trained on how to stay safe online and help tackle bullying, as well as learn more about the tools and resources available to them on Facebook.

- Poland - Digital Harbour[66], in partnership with UNICEF and NASK, is an education programme aimed to develop critical thinking about online content and educate teenagers how to behave safely online and recognise misinformation. The core of this project is an educational platform with training materials for both teachers and students. The project also includes online conferences for teachers as well as Internet Conscious Day, preparing additional materials and organizing a contest for schools.

- Spain and Portugal - Generazión[67], in partnership with Cibervoluntarios.org, INCIBE, UNICEF and Intef, is an educational program aimed to promote online safety and critical thinking among young people ages 14 to 18. Since its launch in 2019 Generazión has reached 9167 students in 116 educational centres. It has delivered 354 workshops and engaged online with 53309 teenagers online through its interactive zone (Zona Interactiva).

- Project deSHAME is a collaboration between Facebook, Childnet (UK), Kek Vonal (Hungary), Save the Children (Denmark) and UCLan (UK), and is co-financed by the European Union. The objective of Project deSHAME (Digital Exploitation and Sexual

---

[62] https://www.facebook.com/help/222332597793306
[63] https://www.facebook.com/safety/resources
[64] https://antibullyingcentre.ie/fuse/
[65] https://diana-award.org.uk/anti-bullying-training/
[66] https://przystanwsieci.pl/
[67] https://www.generazion.org/

Implementation of the ICT Principles

Harassment Among Minors in Europe) is to increase understanding and reporting of online sexual harassment among minors, an emerging area of gendered violence against children, through developing and evaluating youth-led and multi-sector interventions in 3 EU Member States (Hungary, Denmark and UK), and then to transfer this learning throughout Europe.

- In 2019, we launched Stop Sextortion[68], a dedicated hub in our Safety Center[69] developed by Thorn[70], a leading NGO in the fight against child sexual abuse, with resources for teens, caregivers and educators seeking support and information related to sextortion.

**7. Please outline briefly any of your own company initiatives in _media literacy and ethical digital citizenship_, designed to help children and young people to think critically about the content consumed and created on the internet.**

Get Digital[71] includes research-based lessons and resources that help young people develop the skills they need to become empowered digital citizens. Get Digital provides young people, educators, parents and care-givers lesson plans and activities organized around five pillars -- Foundations, Wellness, Engagement, Empowerment and Opportunities-- to help build the core competencies and skills young people need to navigate the digital world in safe ways.
These resources are designed to be used by educators and families both in the classroom and at home. Educator lessons are drawn from the Youth and Media team at the Berkman Klein Center for Internet & Society at Harvard University, which has made them freely available worldwide under a Creative Commons license, as well as lessons from the Greater Good Science Center at University of California, Berkeley.

The Digital Literacy Library[72] is a collection of lesson plans to help young people think critically and share thoughtfully online. The first set of ready-to-use lessons in the library were developed by the Youth and Media researchers at the Berkman Klein Center for Internet & Society at Harvard University under a Creative Commons license. Developed for educators of youth ages 11 to 18, the lessons incorporate over 10 years of academic research by the Youth and Media team, and they reflect the diverse voices of young people from around the world. The lessons address topics like reputation management, identity exploration, cybersecurity and privacy.

We also have a dedicated Youth portal[73] on our Safety Centre.

**8. Please provide details of any advice and support _to encourage parents or teachers to talk to their children_/ pupils about the opportunities and risks arising from their use of the internet.**

---

[68] http://facebook.com/safety/StopSextortion
[69] http://facebook.com/safety
[70] https://www.thorn.org/
[71]  https://www.facebook.com/fbgetdigital/
[72] https://www.facebook.com/safety/educators
[73] https://www.facebook.com/safety/youth

Implementation of the ICT Principles

Get Digital[74] includes research-based lessons and resources that help young people develop the skills they need to become empowered digital citizens. Get Digital provides young people, educators, parents and care-givers lesson plans and activities organized around five pillars -- Foundations, Wellness, Engagement, Empowerment and Opportunities-- to help build the core competencies and skills young people need to navigate the digital world in safe ways.

These resources are designed to be used by educators and families both in the classroom and at home. Educator lessons are drawn from the Youth and Media team at the Berkman Klein Center for Internet & Society at Harvard University, which has made them freely available worldwide under a Creative Commons license, as well as lessons from the Greater Good Science Center at University of California, Berkeley.

The Digital Literacy Library[75] is a collection of lesson plans to help young people think critically and share thoughtfully online. The first set of ready-to-use lessons in the library were developed by the Youth and Media researchers at the Berkman Klein Center for Internet & Society at Harvard University under a Creative Commons license. Developed for educators of youth ages 11 to 18, the lessons incorporate over 10 years of academic research by the Youth and Media team, and they reflect the diverse voices of young people from around the world. The lessons address topics like reputation management, identity exploration, cybersecurity and privacy.

We have a dedicated Parents Portal[76] as well as a Bullying Prevention Hub with tips for parents[77] and educators[78] on our Safety Centre.

**9. Please outline any additional activities or initiatives _not detailed above_ that relate to education and awareness-raising offered by your service or product.**

/

---

[74]  https://www.facebook.com/fbgetdigital/

[75] https://www.facebook.com/safety/educators

[76] https://www.facebook.com/safety/parents

[77] https://www.facebook.com/safety/bullying/parents

[78] https://www.facebook.com/safety/bullying/educators

Implementation of the ICT Principles

In addition to information submitted related to implementation of the ICT Principles, the following supplementary information supplied in either written form or in discussion with companies provides valuable context and information about the functioning and effectiveness of child safety provision.

| |
|---|
| **1. In respect of ICT Principle 1, that companies should "continue work to provide innovative solutions able to support child safety protection tools and solutions", please elaborate on company investment in child safety measures, including research. Elaborate also, where possible, on planned future implementations.** |
| **2. Any further data that companies may be able to provide regarding the functioning of child safety features would be an extremely valuable outcome of this assessment.**<br><br>**Where possible, please provide any available summary data in respect of the following elements. (Stipulate where data should only be presented in anonymised form).** |
| Take up or frequency of use of parental control tools on your product or service?<br><br>Incidence of reporting use/misuse, categorization and frequency of reports on your product or service? How many? By whom? Which problem?<br><br>Kinds of actions taken by the provider for different categories of reports. What was the outcome?<br><br>How do you evaluate the effectiveness of response to reports?<br><br>Privacy settings: the percentage of children who have private profiles, and those who have changed default privacy settings (and how/what did they change), by age, gender and country<br><br>Use of location-based services by children<br><br>Take up and use of education and awareness raising activities undertaken for your product or service? |
| **3. Please detail any additional measures adopted to evaluate the effectiveness of child safety features.** |