



Implementation Questionnaire

January 2017

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 European member states

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*
- Network operators and connectivity providers*
- Online content provider*
- Online service provider*
- Other (please specify):*

5. Person(s) completing the report

Name: ...Julie de Bailliencourt.....

Position:.....Safety Policy Manager EMEA.....

Email:juliedeb@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?

- Yes
 No
 Not applicable (please explain):

If yes, please provide details:

Facebook is a service used by over 1.8 billion people every month across the world. If people see content on Facebook they believe to be inappropriate or abusive, they can report this to our team in a few easy steps. Reporting links are available for every piece of content on Facebook, and our teams have worked hard to make the reporting process as speedy and user friendly as possible. These reporting links are available across all device types (tablet, desktop, and mobile phones).

On Facebook, users have the ability to report a piece of content shown in their newsfeed, report a specific user timeline, or report any other piece of content individually (post, comment, photo, video, group, event, page etc).

Facebook's Help Centre also provides our community with explicit online resources further explaining how to report content on our platform:

<https://www.facebook.com/help/181495968648557/>. Our Help Centre (www.facebook.com/help) also includes additional reporting contact forms, for specialized topics such as memorialization requests, IP infringements and many others.

The Facebook Help Centre also contains additional specialised contact forms for people to get in touch with us and highlight potentially abusive content. This is especially useful for example for people who are not registered on Facebook and wish to report something for the attention of our support teams.

Whenever someone reports a piece of content to us, Facebook always acknowledges receipt of this report, and provides feedback on our team's action after the content was reviewed. This information lives in the support inbox (<https://www.facebook.com/support/>)

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

- Yes
- No
- Not applicable (please explain):

If yes, please provide details of mechanisms in place:

When someone signs up to Facebook, he or she must provide his or her birthdate. If a child indicates that he or she is under 13, Facebook lets the child know we cannot process the registration and if the individual returns later to try again, we let the child know he or she is ineligible to sign up for Facebook. Next to the birth date entry box we also have a link to a dialogue box that explains that we collect birth date to help make sure the user gets the right Facebook experience for his or her age.

This is important because at Facebook we offer stricter default privacy settings for members of the Facebook community who are under 18 years old

In addition to these initial safeguards, Facebook has developed robust Community Standards and rely on our community to report content that may violate those standards.

On Facebook, for certain graphic content that has been reported to us but does not violate our Community Standards, we are also in a position to add an interstitial warning for adults, and age-gate for minors. Adults will see the warning and will have to click further to view the video. Children simply won't be shown the video in question.

In addition, we encourage our community to consider the audience they are sharing with, and behave in a responsible and considerate manner. Facebook offers multiple ways for people to control how and with whom they share, including to smaller restricted audiences. For example people can share and discuss certain topics in closed groups, where the content would not be visible unless the person has specifically been added or joined the group.

Page admins are required to clarify the audience that is the most suitable to interact with their page, and can ensure it becomes invisible to minors (see Screenshot 1 below). We ask page admins to follow our guidelines when it comes to content, and have clearly stated rules specific to regulated goods or services. Page admins have to restrict access to minors when the page in question promotes the private sale of alcohol, tobacco, adult products, firearms etc.

Pages promoting the private sale of regulated goods or services (including firearms, alcohol, tobacco, or adult products) must restrict access to a minimum age of 18.

We have strict guidelines when it comes to advertising policies, particularly for content that may be targeting under 18's. These standards can be consulted on <https://www.facebook.com/policies/ads/#>. Ads that fail to follow our age targeting requirements will be disabled (<https://www.facebook.com/help/256048321073744>)

Apps must be gated to 18+ where they involve content unsuitable for minors (section 3.8 of the Statement of Rights and Responsibilities). Extensive information is available to developers on our developers portal. Consult <https://developers.facebook.com/policy> for more information on policies.

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
- How to block or restrict access to content
- How to report or flag content as inappropriate
- Safe searching
- 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.):

Facebook provides extensive information on how to manage interaction with pages, content and individuals on Facebook: from following/unfollowing to unfriending, hiding, or even blocking. Moreover we have created extensive resources on how report abusive content and get help from our team.

These resources are available in our Help Centre (www.facebook.com/help), Safety Centre (www.facebook.com/safety), as well as from the Privacy Shortcuts and Safety settings (<https://www.facebook.com/settings?tab=privacy>). Resources are available in a number of formats, from short videos in our Safety Centre, to comprehensive FAQs in our Help Centre, to PDFs available to download etc. In all cases, these resources are made available in a large number of languages (50+) and user friendly format.

Facebook also regularly publishes tips and advice in language from our Facebook Safety page.

In December 2016 Facebook also launched a new online resource for parents, the Parents Portal, available in 50+ languages (www.facebook.com/safety/parents). This practical guide aims to provide tips and resources to parents who are new to Facebook, or whose teens are on Facebook.

4. Where is your company's Acceptable Use Policy (AUP) located?

Our Terms of Service can be found online <https://www.facebook.com/legal/terms> and govern Facebook's relationship with our users or others who interact with Facebook. We have also developed more extensive resources around the type of content that is allowed on our platform, and these Community Standards are readily available here: <https://www.facebook.com/communitystandards>. Our Community Operations team will often refer people to the Community Standards page, in order to draw their attention to our existing guidelines, and provide more context as to some of the decisions we may have reached with regards to potentially abusive content.

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

- Yes
- No
- Not applicable (please explain):

If yes, please identify relevant policy:

Facebook's Community Standards are available on www.facebook.com/communitystandards. This page is heavily emphasized via our Help Centre, Safety Centre etc. We also encourage our users to refer to this page, especially when reporting content, or when we have removed content found to be abusive. In May 2015 we updated our Community Standards page, to provide additional context and detail as to the type of content we do not allow and educate our community about the updated standards. Our goal is to provide as much clarity as possible to our community around our policies.

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:

The vast majority of the content posted on Facebook is by nature positive, benign and uncontroversial. At times, our community will report potentially abusive content to us.

Whenever Facebook reviews a piece of content that has been reported for being abusive or harassing in nature, we communicate very clearly to the person who made the report by providing them with updates in their Support Inbox.

The reporting person will follow the progress of their report: they will be updated when we have assessed their report, and will have full visibility on the actions that were taken by our team.

Facebook will also notify the reported user if we have assessed that they have posted content that is against our Community Standards. In such case, the person will receive a notification that we have removed some of their content, with some more information about the type of content or behaviour that we prohibit. In some cases, we will also ask them to go back to their account and remove any other similar material they may have on their timeline that would be against our terms of use.

We also hold Facebook group admins and page admins to similar standards, and strive to educate everyone about sharing content in a respectful environment.

People who continuously post abusive content or behave in an abusive way may be

prevented from using certain Facebook features (such as the ability to upload a photo or send a message for example), or lose access to their Facebook account altogether.

If people lose access to their Facebook account, page or group, we have put in place an appeals process for further investigation and a final decision from our team.

In a small number of cases, there are more severe consequences for people who engage in extremely abusive or illegal behaviour. For example we simply do not tolerate predatorial behaviour towards children, and accounts found to be engaging in such behaviour will be swiftly removed and not reinstated. In certain circumstances, we may also bring such accounts to the attention of law enforcement.

Facebook values authentic identity, and does not allow fake accounts. These accounts will be removed with all of their associated content. A proof of identity may be required during the appeals process, after which a user may regain access to their timeline.

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:

When teens over the age of 13 are registered on Facebook, they have full control over their account. Our philosophy is to empower parents to have conversations with their child about the online space, and promote responsible online behaviour from all. We aim to fully equip parents with the tools and conversation starters they need, and have worked with safety experts to provide parents and teens with a range of resources, to help them answer questions they may have <https://www.facebook.com/safety/parents> and <https://www.facebook.com/safety/bullying/parents> . Our dedicated Parent Portal, launching in December 2016, was developed with parents in mind and to support them in the best possible way.

For example on Facebook, we have come up with several tools and conversation starters to talk about bullying. These are also suitable whether the parent identifies that their child could be bullied or may be bullying someone else.

<https://www.facebook.com/safety/bullying/parents/mychildisbeingbullied>

In December 2016 we also launched the Parents Portal, a dedicated resource available in 50+ languages, for parents who are new to Facebook or whose teens are on Facebook (www.facebook.com/safety/parents). This practical collection of tips and useful links aims to empower parents to initiate a conversation with their children about the online world.

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

As mentioned, we have created easy to understand resources available in 50+ languages in our Safety Centre (www.facebook.com/safety) and Help Centre (www.facebook.com/help), including our summary of FAQs for parents and educators: <https://www.facebook.com/help/441374602560317/>.

As previously mentioned, in December 2016 Facebook launched the Parents Portal, a dedicated resource available in 50+ languages, for parents who are new to Facebook or whose teens are on Facebook (www.facebook.com/safety/parents). This practical collection of tips and useful links aims to empower parents to initiate a conversation with their children about the online world.

3. In relation to parental controls, which of the following educational and information resources to do you offer?

(tick as many as apply)

- 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*

Tools for parents and educators: <https://www.facebook.com/help/441374602560317/>

Parents portal: www.facebook.com/safety/parents

[Please provide details including links or screenshots as relevant]

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?

--

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.

Our Facebook Community Standards address describe acceptable behavior and detail the type of content that we consider inappropriate on both platforms.

These extensive documents include a whole range of inappropriate content such as direct threats, nudity, graphic content, bullying and harassment, sexual exploitation, fraud, spam, intellectual property infringements, and including Facebook's real name requirements.

<https://www.facebook.com/communitystandards>

When someone comes across content they believe is inappropriate on Facebook, they can report it to our support teams using the reporting links available on the site. Reports are then prioritized in order to ensure the most appropriate team reviews them. We prioritize by looking at potential real world harm, and aim to move fast on critical reports from users. (Refer to ICT1 for full report mechanism overview).

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).

As previously mentioned, 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).

Users can report a piece of content shown in their newsfeed, report a specific user timeline or report any other piece of content individually (post, comment, photo, video, group, event, page etc). Our Help Centre offers additional ways for people to report content to us.

Reporting is quick, easy, confidential, and only takes a few seconds. It is important that people report content to us using the option that is the closest to the type of abuse they are seeing. This helps us assess the potential severity of the issue, and also identify the team that is best positioned to handle the report (specialisation, language and market expertise).

We have spent the last twelve years improving our robust reporting mechanisms, and have also ensured the support we provide is of high quality. While we do not share information related to our internal turnaround times, our support inbox provides everyone with full transparency on how quickly their individual reports are being reviewed. In general, someone in our team will look at most reports within a few days. We strive to get to the most urgent reports in a matter of hours. It is important for our teams to get first to the reports that have a credible risk of real world harm.

Our Community Operations teams are based in several locations across the globe. This allows us to continuously support people who need our help, regardless of time zone.

We rely on smart technology to help us take action against potential phishing links, scammers, phishers or fake accounts, but reports will mainly be reviewed by a team of real people.

[Please provide details including links or screenshots as relevant]

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

- On each page of the website/service*
- Close to the point where such content might be reported*
- 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)

- Only registered user/profile in which content is located*
- 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):*

Everyone can report a piece of content to our team, whether they are registered on Facebook or not.

5. Which of the following kinds of content can users report?

All content types (individual profiles, groups, events, pages, videos, photos, comments, status updates, messages etc). <https://www.facebook.com/help/263149623790594>

6. Which of the following information do you provide to users?

(tick any that apply)

- Advice about what to report*
- Advice about how to make a report*
- Pre-defined categories for making a report*
- How reports are typically handled*
- Feedback to users*
- Other website/external agency for reporting abuse/ misuse content?*
- 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

In addition to being able to report any piece of content published on Facebook, people have the ability to go to Facebook's Help Centre which provides our community with explicit online resources further explaining how to report content on our platform:

<https://www.facebook.com/help/181495968648557/>

The Facebook Help Centre also contains additional specialised contact forms for people to get in touch with us and highlight potentially abusive content. This is especially useful for example for people who are not registered on Facebook and wish to report something for the attention of our support teams

(<https://www.facebook.com/help/contact/274459462613911>)

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*
- Link or button for external national or regional INHOPE hotline*
- Emergency services*
- Law enforcement agency*
- Other external agency (please specify):*

We work with law enforcement to help people on Facebook and Instagram stay safe. This sometimes means providing information to law enforcement officials that will help them respond to emergencies, including those that involve the immediate risk of harm, suicide prevention and the recovery of missing children.

When we receive and verify a report of child exploitation on the site (either material or illegal contact), we immediately take action. We relay every offending image, along with relevant account information, to the U.S. National Center for Missing and Exploited Children (NCMEC). When apparent solicitation of minors is identified, we report this also to the relevant authorities. We work with the CEOP Command of the UK National Crime Agency, the Internet Watch Foundation, and a number of child safety organisations worldwide. These organisations have a dedicated channel to notify us of possible safety issues and request assistance from us.

We cooperate with local, national and international authorities, to bring offenders to justice. It is incredibly rewarding when we hear back from these groups about a report from us that has resulted in the safeguarding of a young person and enforcement against an offender.

We also use technology to help combat the spread of exploitative material. One of the most effective technologies is PhotoDNA, created by Microsoft and Dartmouth University. When someone uploads an image to Facebook, it is checked against signature lists for known child exploitation material. We report all apparent instances of child exploitation appearing on our site from anywhere in the world to the National Center for Missing and Exploited Children (NCMEC), including content drawn to our attention by government requests. In order to optimise PhotoDNA’s detection capability, we share our list of identified child exploitation material with other Internet companies.

We disclose account records solely in accordance with our Terms of Service and applicable law, including the federal Stored Communications Act (“SCA”), 18 U.S.C. Sections 2701-2712. Accredited law enforcement single points of contact (SPOCs) can submit requests under RIPA to a dedicated online request system at www.facebook.com/records . Requests relating to a child exploitation or safety matter are processed as a matter of priority.

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

Over the past twelve years, we have developed robust reporting flows and mechanisms, available to everyone and in 50+ languages. Our community can report potentially abusive content at any time, using the reporting links available throughout our platforms.

As mentioned, we prioritise reports based on their potential severity, the risk of real world harm, and whether minors are involved. As such, potential child abuse is something we want to investigate as quickly as possible. Our support teams are dedicated to reviewing content 24/7, and work across the globe to ensure we are always available. Most reports are reviewed within a few days, and for the most critical, within a few hours.

Upon assessing that the reported content is indeed child exploitation material, our team would immediately take action. The content is taken down and the account responsible for sharing it is disabled and reported to NCMEC (the National Centre for Missing and Exploited Children), where it is further referred to law enforcement. Our team of trained child safety experts may also further investigate content associated with the abusive account, such as friends, groups etc.

We have a dedicated page in our Help Centre offering additional support and information for people who may have been exposed to child sexual exploitation material:

<https://www.facebook.com/help/189165674568397> .

Our community can also report convicted sex offenders to us, using a special contact form in our Help Centre: <https://www.facebook.com/help/210081519032737> and

<https://help.instagram.com/131932550339730> .

Convicted sex offenders are not allowed on our platforms, and upon review, their accounts will be removed.

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)

Links to relevant child welfare organizations/specialist providers of advice

Other confidential helplines/support services

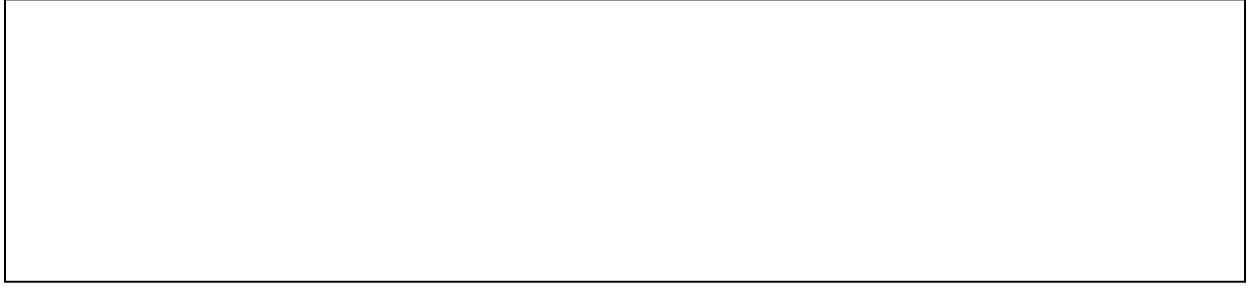
Law enforcement agencies

INHOPE

Other (please specify):

Links to relevant child welfare organizations or confidential helplines and hotlines can be found throughout our Safety Centre (www.facebook.com/safety) and Help Centre (www.facebook.com/help). We are continuously working to improve all of these resources and make them as user friendly as possible, in a broad range of languages.

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?



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 access, collection, sharing and further use of data from minors under the age of 18 when utilizing your product or service?

This information can be found in our Data Use Policy.

https://www.facebook.com/full_data_use_policy

<https://www.facebook.com/about/privacy>

2. Are distinct privacy settings deployed to prevent access to information on for users under the age of 18?

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 work hard to help keep people on Facebook safe. For minors, we've designed many of our features to remind them of who they're sharing with and to limit interactions with people they don't know.

For example, we provide minors with specific education about what it means to post publicly. We also protect sensitive information, such as minors' contact info, school and birthday, from appearing in search to a public audience. Additionally, we take steps to remind minors that they should only accept friend requests from people they know. Also, with regard to messaging, the default setting is more restrictive in order to prevent teens receiving messages from strangers while allowing them to message friends, friends of

friends and other people they may know. Another feature is the Tag Review tool that is on by default for teens, before a tag is posted it needs to be accepted by the person. Finally, it's important for minors in particular to think before they share their location, location sharing is off for them by default. When either an adult or minor turns on location sharing, we include a consistent indicator as a reminder that they're sharing their location.

When a teenager creates a Facebook account, it will benefit from certain behind-the-scenes protections, alongside stricter default privacy settings.

For example:

- Minors do not have public search listings created for them, and their email and phone number may never be set to 'Public'
- The 'Public' audience setting is not available until they have completed extensive education around what it means to post publicly.
- Messages sent to minors from adults who are not friends (or friends of the minor's friends) are filtered out of the minor's inbox.

More information about under 18's and privacy:

<https://www.facebook.com/help/www/473865172623776?rdrhc>

Please identify default settings for each age category of under 18s, as relevant:

We have one age category for teens, which is 13-17. The above settings apply to them by default.

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

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

- On each page of the website/service
- At each point where content may be posted
- 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):

[Please provide details including links or screenshots as relevant]

We created a new privacy education and resource Centre called Privacy Basics (<https://www.facebook.com/about/basics/>), which helps people manage their information on Facebook through a series of over fifteen interactive modules. The modules are based on the top questions people ask in the Help Centre, and are grouped into four topical sections:

- What Others See About You: Includes information on choosing the audience for posts, deleting posts, account deactivation and deletion, and how tagging works.
- How Others Interact With You: Explores what information people can post on your timeline, who can like or comment on things you post, and how untagging, unfriending, and blocking work.
- What You See: Explains how to change what content appears in your News Feed or the kinds of ads you see.
- How to Keep your Account Secure: Helps you take the right steps to secure your account on Facebook.

Facebook Privacy Basics is designed in a colorful, engaging way that appeals to young people and adults alike, and is easy to read and understand. Privacy Basics layers on top of our Help Centre, which provides additional details around how to use and benefit from our privacy controls: <https://www.facebook.com/help/>.

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, last year we launched our first version of Privacy Checkup, which reminds people who have been posting publicly for some time that they are, in fact, posting publicly— and to make sure they're sharing with their intended audience. We built upon this effort later in the year when we launched the second version of Privacy Checkup, which walks people through a few quick steps to help make sure they're sharing information with the people they want. When people use the Checkup, they'll be able to review the audience they're posting to on Facebook, which apps they're using, and the privacy of key pieces of information on their profile. The tool is available anytime in Privacy Shortcuts on Desktop, and we are working to make it available on Mobile as well.

<https://www.facebook.com/settings?tab=privacy>

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 encourage open communication between children and their parents about safe and responsible use of the Internet, and provide important resources to facilitate these conversations through our Safety Centre: <https://www.facebook.com/safety>. Anyone under 18 who uses Facebook will have more restrictive privacy settings than adults as a default.

For example:

- Minors do not have public search listings created for them, and their email and phone number may never be set to 'Public'
- The 'Public' audience setting is not available until they have completed extensive education around what it means to post publicly.
- Messages sent to minors from adults who are not friends (or friends of the minor's friends) are filtered out of the minor's inbox.

Please find below a list of some of the main controls we offer to everyone who uses Facebook:

- **Inline audience controls for your posts:** Our inline audience controls allow people to customise the audience for the content they post. People can choose to share with one particular friend or family member, friends, friends of friends, or publicly. People can also customise lists to share with particular groups of friends.
- **Inline audience controls for other information on Facebook:** Inline audience controls are also available for other information people share on Facebook, including information people share in the "About" section of their Timeline—such as education, contact information, and life events.
- **Friends default:** People who are new to Facebook now start with a default setting of "Friends" for their first post. First-time posters will also see a reminder to choose an audience for their first post, and if they don't make a choice, it will be set to Friends.
- **Privacy Checkup v1:** When people have chosen to post publicly for awhile, we may remind them that they're posting publicly to make sure they're sharing with their intended audience.
- **Privacy Checkup v2:** This tool walks people through a few quick steps to help make sure they're sharing information with the people they want. When people use the Checkup, they'll be able to review the audience they're posting to on Facebook, which apps they're using, and the privacy of key pieces of information on their profile. The tool is available anytime in Privacy Shortcuts on Desktop, and we are working to make it available on mobile as well.

- **Activity Log:** The Activity Log is a private list of a person’s posts and activity on Facebook, from stories and photos they’ve been tagged in to connections they’ve made – such as when they’ve like a Page or added someone as a friend. Activity Log also enables people to change the audience for their posts, untag themselves in photos, and delete or hide information they’ve shared.
- **Tag Review:** Tag review is an option that lets people approve or dismiss tags that others add to their posts. When Tag review is turned on, anytime someone tags something you posted, that tag won't appear until you approve it.
- **Timeline Review:** Timeline Review allows people to approve or hide posts by others before they become visible on their Timeline. These posts will be hidden from Timeline, but can still appear News Feed, search, and other places on Facebook. When people you’re not friends with tag you in a post, the posts automatically go to Timeline review. To review tags by friends, people should turn on Timeline review from the “Timeline and Tagging” section in the Settings menu.
- **View As:** This tool helps you see what your profile looks like to other people. People can see what their profile looks to the public, and can also see how their profile appears to a specific person, like a friend or colleague. To use this tool, people can click on the ellipses next to the “Activity Log” button on their Timeline.
- **Download Your Information (“DYI”):** People can request and obtain a report of the data they have provided to Facebook using the “Download Your Information” tool. This tool includes information that is also available to people in their accounts and Activity Log, such as posts they’ve shared, messages, and photos. It also includes information that is not available simply by logging into people’s account, like the IP addresses that are logged when people log into or out of Facebook, and more. To download your information, people can go to their Settings and click “Download a copy of your Facebook data.”
- **Ad Preferences Tool:** Through our Ad Preferences tool, people can learn more about why they see certain ads on Facebook and also manage the preference categories we have associated with them. We are in the process of rolling out Ad Preferences to a global audience.
- **People First advertising control:** This advertising control lets people opt-out of interest-based advertising everywhere they use Facebook. Once someone opts out – whether through a preference in their device settings or through the Digital Advertising Alliance opt out— we will apply the choice they have made *everywhere* they use Facebook.

We recently created a new privacy education and resource Centre called Privacy Basics (<https://www.facebook.com/about/basics/>), which helps people manage their information on Facebook through a series of over fifteen interactive modules. The modules are based on the top questions people ask in the Help Centre, and are grouped into four topical sections:

- What Others See About You: Includes information on choosing the audience for posts, deleting posts, account deactivation and deletion, and how tagging works.

- How Others Interact With You: Explores what information people can post on your timeline, who can like or comment on things you post, and how untagging, unfriending, and blocking work.
- What You See: Explains how to change what content appears in your News Feed or the kinds of ads you see.
- How to Keep your Account Secure: Helps you take the right steps to secure your account on Facebook.

Facebook Privacy Basics is designed in a colorful, engaging way that appeals to young people and adults alike, and is easy to read and understand. Privacy Basics layers on top of our Help Centre, which provides additional details around how to use and benefit from our privacy controls: <https://www.facebook.com/help/>.

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, last year we launched our first version of Privacy Checkup, which reminds people who have been posting publicly for some time that they are, in fact, posting publicly— and to make sure they’re sharing with their intended audience. We built upon this effort later in the year when we launched the second version of Privacy Checkup, which walks people through a few quick steps to help make sure they're sharing information with the people they want. When people use the Checkup, they'll be able to review the audience they're posting to on Facebook, which apps they're using, and the privacy of key pieces of information on their profile. The tool is available anytime in Privacy Shortcuts on Desktop, and we are working to make it available on Mobile as well.

[Please provide details including links or screenshots as relevant]

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.

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
- Teenagers <18s
- Parents and carers
- Teachers and other adults
- Others (please specify):

2. Which of the following topics are included within your own company educational materials?

(tick any that apply)

- Online safe behaviour
- Privacy issues
- Cyberbullying
- Download and copyright issues
- Safe use of mobile phones
- 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
- Notification by email / on-screen statement / other means when product or contract is purchased or first registered
- Prominent notifications, resources or pop ups on website
- Helpdesk (telephone or online)
- Other (please specify): .online help centre, downloadable resources available in Facebook's safety centre, printed material distributed via safety partners.

.....

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

There are many resources and excellent partners throughout Europe and across the world. We endeavor to developing relationships with as many as these safety NGOS as possible.

In 2009 Facebook created it's own Safety Advisory Board, comprising of several expert organisations located in the US, UK, India etc:

(https://www.facebook.com/help/222332597793306?helpref=faq_content).

Here is a snapshot of some of the organisations listed in our Safety Centre.

Global resources: FOSI, Child Helpline International, INHOPE/INSAFE, National Centre to End Domestic Violence.

UK: The Diana Award, Childnet, UK Safer Internet Centre, Stonewall, Internet Matters

Germany: FSM, Jugendschutz, Klicksafe

France: Net Ecoute/Internet Sans Crainte, protection e-enfance, AFPI

Cyprus: Safer Internet CyberEthics

Portugal: MiudosSegurosNa.net

Austria: Safer Internet.at

Spain: Pantallas Amigas, Fundacion ANAR, Alia2, GSIA, Padres 2.0

Greece: SaferInternet4kids, Hamogelo Smile of a Child

Denmark: Borns Vilkar, Save the Children

Italy: Telefono Azzurro, Save the Children

Ireland: Webwise, Spunout.ie,

Sweden: BRIS, Tjejzonen

Belgium: Child Focus

Luxembourg: BEE Secure
 Czech Republic: Safer Internet Centre
 Bulgaria: Safenet

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?

ICT Coalition
 UKCCIS
 Alliance to Better Protect Children Online.

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.

ENABLE is the acronym for the [European Network Against Bullying in Learning and Leisure Environments](#). The project started in October 2014 and is co-funded by the DG Justice of the European Commission. Associate partners are Facebook, Twitter, Ask.fm and Vodafone and Kaspersky Lab. ENABLE is also supported by Microsoft, Council of Europe, Icelandic Red Cross and Liberty Global. The project was implemented in a half dozen countries across Europe, and worked with 8,000 young people aged 11-14 years, and empowered 2,000 parents and teachers, and was integrated in at least 30 schools. The project is based on the premise that well-being in today's information and knowledge society calls for sound social and emotional skills, built through a deeper understanding and a responsible approach to on- and offline social interactions. Last month, Facebook hosted the ENABLE Hackathon which explored with young people the issues surrounding on and offline bullying, and helped young people to understand the dynamics behind bullying and worked with the young people in teams to find creative solutions to stop bullying.

Diana Award: We have worked with The Diana Award for the past six years, the charity was established as a legacy to Princess Diana who strongly believed that young people had the power to change the world. As part of the partnership, we support the Diana Award in training their 'Anti-Bullying Ambassadors' in schools across the UK, this peer-to-peer model is very effective in tackling bullying and giving young people confidence to speak out. We also support the charity in the production of national events and during UK Anti-Bullying Week which takes place in November each year where we train over 500 young people and teachers on online safety on Facebook. In February 2016, we launched a new resource ['Anti-](#)

[Bullying Activism on Facebook'](#) - a guide for schools who would like to set up their own anti-bullying initiatives on Facebook.

ChildNet Digital Leaders Programme: Launched in September 2015, the [Childnet Digital Leaders Programme](#) aims to empower young people to champion digital citizenship and digital creativity within their schools and to educate their peers, parents and teachers about staying safe online. The programme offers pupils structured training and ongoing support from Childnet's expert team, helping make e-safety learning fun and effective and ensuring that schools deliver an outstanding whole school community approach to e-safety. We have supported the programme in collaboration with the European Union, the programme connects young people with other Childnet Digital Leader schools across the UK, and gives young people opportunities to chat with top tech companies and have a say in creating a better internet for the future.

We support Safer Internet Day across Europe and the world as well as the efforts of a large range of safety experts and NGOS in country, from INHOPE to Child Helpline International.

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.

We've worked with schools across the UK and Spain and leading UK educational Think Tank, The Education Foundation, to develop a guide for teachers on how they can use Facebook in the classroom as a learning tool, as well as outlining all the safety features we have on the site.

<http://www.ednfoundation.org/wp--content/uploads/Facebookguideforeducators.pdf>

http://www.youtube.com/watch?v=IE_ZDhUkRwg

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

Tips for parents:

<https://www.facebook.com/safety/bullying/parents>

Tips for teens:

<https://www.facebook.com/safety/bullying/teens>

Tips for teachers:

<https://www.facebook.com/safety/bullying/educators>

9. Please outline any additional activities or initiatives *not detailed above* that relate to education and awareness-raising offered by your service or product.

We work closely with stakeholder, schools and NGOs to promote digital literacy.

We create regular videos for young people to raise awareness about all of our safety tools which we share with partners. These can be found here:

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.

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?

n/a

Incidence of reporting use/misuse, categorization and frequency of reports on your product or service? How many? By whom? Which problem?

Kinds of actions taken by the provider for different categories of reports. What was the outcome?

How do you evaluate the effectiveness of response to reports?

Our support teams are constantly evaluating whether or not Facebook is able to provide a high quality answer to people who need our help, and within a reasonable turnaround time. These ongoing checks continuously inform our support operations to ensure our community is happy with the service provided.

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

Use of location-based services by children

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.