GUIDE TO USING THE CHILD ONLINE SAFETY ASSESSMENT TOOL

EMPOWERING TECHNOLOGY COMPANIES TO PROMOTE A SAFE ONLINE ENVIRONMENT FOR CHILDREN

© UNICEF/BANA2014-01597/Mawa
ACKNOWLEDGEMENTS

Prepared by the UNICEF Child Rights and Business Unit

(Note: Names of stakeholders involved in tool development to be added in final version.)

FEEDBACK AND QUESTIONS

Your feedback and questions about the Child Online Safety Assessment will be vital to improving the tool. We encourage you to send comments and queries to <CSR@unicef.org>.

All rights to this guide remain with the United Nations Children’s Fund (UNICEF). No part of this document may be replicated or redistributed without the prior written permission of UNICEF.

A reference to a non-UNICEF website does not imply endorsement by UNICEF of the accuracy of the information contained therein or of the views expressed.

February 2016

Guide to Using the Child Online Safety Assessment Tool

CONTENTS

ACKNOWLEDGEMENTS .............................................................................................................. 2

ABBREVIATIONS ..................................................................................................................... 4

GLOSSARY ................................................................................................................................. 5

INTRODUCTION ........................................................................................................................... 7

Objectives and development process .......................................................................................... 7

Working with stakeholders ............................................................................................................ 9

GUIDANCE TABLES FOR THE CHILD ONLINE SAFETY ASSESSMENT TOOL .................. 16

1. Legal – Ensuring corporate policies and management processes comply with applicable legislation ..... 17
2. Human Rights and Corporate Responsibility (Human Rights & CR) – Integrating child rights considerations into all appropriate corporate policies and management processes ..... 22
3. Human Resources – Working to make sure all employees are aware of child rights and exhibit appropriate behaviours ..... 28
4. Procurement – Working with suppliers to align values, expectations and performance ..... 30
5. Product Development – Creating safer and age-appropriate online environments through product development, in use, and through interaction with customers and users ..... 31
6. Commercial – Ensuring marketing, sales and products and services promote child online safety ..... 38
## ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COPPA</td>
<td>Children’s Online Privacy Protection Rule</td>
</tr>
<tr>
<td>CSAM</td>
<td>child sexual abuse material</td>
</tr>
<tr>
<td>ICT</td>
<td>information and communication technology</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union (United Nations)</td>
</tr>
<tr>
<td>N/A</td>
<td>not applicable</td>
</tr>
<tr>
<td>UNICEF</td>
<td>United Nations Children’s Fund</td>
</tr>
</tbody>
</table>
### GLOSSARY

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>adolescent</strong></td>
<td>UNICEF and other United Nations agencies define ‘adolescence’ as age 10–19. For international law, anyone under 18 is considered to be a child, whereas those 18–19 years old are adults, unless the age of majority is attained earlier under national law. In the context of children’s rights, it is vital for business to consider the unique needs of adolescents, who are in a transitional phase separate from both early childhood and adulthood. As adolescent girls and boys grow, they take on additional responsibilities, experiment with new ways of doing things and push for independence – developing values and skills that have great impact on their well-being. For information and resources on adolescents and young people, see &lt;www.unicef.org/adolescence&gt;.</td>
</tr>
<tr>
<td><strong>child</strong></td>
<td>As stated in the Convention on the Rights of the Child article 1, “a child means every human being below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier.”</td>
</tr>
<tr>
<td><strong>child sexual abuse material (CSAM)</strong></td>
<td>‘Child sexual abuse material’ refers to representation – by any means, including but not limited to photography, video, drawings, cartoons, text and live streaming – of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes. Although there is no internationally agreed definition of ‘child abuse material’, the Child Online Safety Assessment tool and guidance use the term as defined above, based on the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, article 2. For the purposes of this publication, the term is preferred over ‘child pornography’ because it leaves no doubt that abuse and exploitation are involved.</td>
</tr>
<tr>
<td><strong>cyberbullying</strong></td>
<td>International law does not define ‘cyberbullying’. For the purposes of this guide, it is defined as behaviour that is harmful or intended to cause harm, occurs repeatedly, and involves an imbalance of power that prevents the victim from challenging or ending the behaviour. Cyberbullying can involve direct approaches, such as chat or text messaging; semi-public tactics, such as posting a harassing message on an e-mail list; and public communication, such as creating a website devoted to making fun of the victim. Children have reported that bullying online is an important issue for them. While more bullying takes place offline than online, information and communication technologies provide new, more invasive and anonymous opportunities for children and young people to bully others.</td>
</tr>
</tbody>
</table>
**grooming**

Online grooming is the process by which an individual befriends a young person for online sexual contact, sometimes with the involvement of webcams that allow ‘sharing’ of the exploitation among networks of child sex abusers, and sometimes extending to a physical meeting to commit sexual abuse. The areas of cyberspace that enable abusers to groom potential victims include chat rooms, social networking sites and instant messaging.

The term ‘grooming’ has not been defined in international law; some jurisdictions use the term ‘luring’.

---

**notice and takedown**

Operators and service providers are sometimes notified of suspect content online by customers, members of the public, law enforcement or hotline organizations. ‘Notice and takedown’ procedures refer to a company’s processes for the swift removal (‘takedown’) of illegal content, defined according to the jurisdiction, as soon as it has been made aware (‘notice’) of the presence of illegal content in its services.

---

**parental control tools**

‘Parental control tools’ are software-based programs that allow users, typically parents, to control some or all functions of a computer or other device that can connect to the Internet. These programs are usually password protected.

Some control tools can limit access to particular types or classes of websites or online services; others also provide scope for time management, i.e., the device can be set to have access to the Internet only during certain hours. More advanced versions can record all texts sent or received from a device.

Control tools need to strike a balance between the right to protection from all forms of violence and exploitation, and a user’s rights to information, freedom of expression, privacy and non-discrimination, as defined in the Convention on the Rights of the Child. It is unlikely ever to be possible to remove all the risks to children that exist in the online environment. Moreover, beyond a certain point, attempting to do so could threaten the very essence of the Internet and its multiple benefits.

---

**young people and youth**

For the purposes of the Child Online Safety Assessment tool and guide, ‘young people’ is used as a generic term. UNICEF and other United Nations agencies define ‘youth’ as age 15–24.
INTRODUCTION

Information and communication technologies (ICTs) are providing children with tremendous opportunities to learn, share and communicate, including access to information about social services, health and educational resources, and empowering children to assert their rights and express their opinions. But despite the profound benefits, when using ICT devices and platforms to access the Internet, children may face such risks as violations of their privacy and exposure to inappropriate and potentially harmful content or contact.

The Guide to Using the Child Online Safety Assessment Tool supports businesses in preparing for and completing an assessment of their impacts related to children. It describes the purposes, background and functions of the Child Online Safety Assessment Tool, and offers detailed instructions and advice for using the tool.

Objectives and development process

The Child Online Safety Assessment Tool is designed to support ICT companies in assessing how children’s rights can be more effectively integrated into their operations, and aims to empower companies to strengthen their child protection policies, codes of conduct and due diligence processes.

This Excel-format tool has been built with inputs from a wide range of stakeholders, including ICT companies across a variety of sectors (online gaming, Internet service providers, social media, search engines and others), industry associations, non-governmental organizations that specialize in child rights for the ICT sector, independent human rights consultants, academics and media experts.

The three primary objectives are to:

1. Ensure companies understand the core issues and impacts to consider when assessing their management of child rights and the Internet.
2. Offer an easy-to-use and comprehensive self-assessment of a company's management of and impact on children’s rights online.
3. Uncover strengths and weaknesses in managing child rights policies and practices, and build corrective plans where needed to adjust management practices.

Children’s use of technology to access the Internet is continuously increasing. In Brazil, for example, children aged 10–14 were the largest group of new Internet users, in absolute terms, between 2005 and 2011.\(^1\) Recent studies in the United Kingdom show that the presence of tablets at home increased significantly for children 5-15 years of age, from 51 per cent in October 2013 to 71 per cent in October 2014.\(^2\)

A 2014 study by The Marketing Store and Kidsay in the United States, showed that 58 per cent of children aged 8–11 accessed the Internet daily, and 71 per cent used it at least three days a week. Additionally, it showed that 75 per cent of children aged 8-11 use more than one electronic device at the same time.\(^3\) Studies in Australia show that 60 per cent of children aged 5–8 and 96 per cent of those aged 9–12 use the Internet.\(^4\)

---

\(^2\) Ofcom, Children and Parents: Media Use and Attitudes Report, October 2014, pg. 23.
Companies in the technology industry – including software, application and game developers, mobile operators, Internet service providers, search engines and social media – are often engaged in online services, solutions and applications businesses that are directly targeted to reach children as consumers. The increase in technology usage among children has brought on new and more complex challenges for all stakeholders, including the ICT companies that develop and offer products, children using these products, and the families and educators looking to support and protect children.

To support businesses in addressing the challenges, the updated Guidelines for Industry on Child Online Protection were developed by ITU and UNICEF in consultation with business and civil society and published in 2014. The guidelines provide advice on how companies can help ensure children’s safety when using the Internet or any of the associated technologies or devices that can connect to it, including mobile phones and game consoles. and recommend that companies proactively support children’s digital citizenship, civic participation, education and access to information and communication technology.

Building on this work and other efforts to safeguard children online, the Child Online Safety Assessment Tool offers companies with an easy-to-use, Excel-format self-assessment tool. This tool has been built with inputs from a wide range of stakeholders, including industry associations, leading ICT companies across a variety of sectors, non-governmental organizations that specialize in child rights for the ICT sector, independent human rights consultants, academics and media experts.

The following international guidelines were used as the foundation for developing the assessment criteria and questions:

- GSMA policies and guidelines, <http://www.gsma.com>

---

Working with stakeholders

Engaging with both internal and external stakeholders – before, during and after the assessment – will be an essential part of preparing for the evaluation, making sure the company’s answers to the self-assessment questions are accurate and comprehensive, and following up on the results.

It is important that sufficient regional and in-country stakeholders are included to represent high-value and high-risk regions, as well as the diversity of locations where your company operates. To begin this process, you will need to map the internal stakeholders who are relevant and necessary to complete the assessment, according to both their function and their location. This involves simultaneously considering each factor, for example:

<table>
<thead>
<tr>
<th>Location</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>Corporate social responsibility</td>
</tr>
<tr>
<td>Regional</td>
<td>Human resources</td>
</tr>
<tr>
<td>In country</td>
<td>Marketing, sales and procurement</td>
</tr>
<tr>
<td></td>
<td>Operational or technical departments</td>
</tr>
</tbody>
</table>

Additionally, companies should consider conducting a number of pre-assessment interviews (phone, email, or face to face) with a range of external stakeholders who can provide expertise on child rights for your industry and/or company. These stakeholders will be those who understand the risks, issues and potential solutions where the business operates, and could include:

- International organizations and agencies
- National and local non-governmental organizations or charity project partners
- Government entities related to child protection
- National bodies related to Internet safety
- Global and/or national industry bodies, such as associations and trade unions
- Suppliers and business partners throughout the value chain.

Questions to ask during the pre-assessment interviews could include:

- What are the known primary child rights impacts in the industry?
- What are the current strengths and weaknesses in managing child rights (in regard to the company or sector)?
- What key issues are not adequately being addressed by the company (or sector) and which issues pose the biggest risk to children?
- Are there new or emerging issues that are currently unmanaged or difficult to manage?
- Are there region-specific issues or trends you feel are important to highlight (in regard to the company or sector)?
How to conduct the Child Online Safety Assessment

There are two parts to the Child Online Safety Assessment: (1) the Excel-format tool and (2) this guidance document. The tool is designed to make it easy to answer questions, and store the results and related evidence generated during the self-assessment. This PDF-format guide for using the tool is set up as a companion to the worksheets. Both the tool and the guide are available at the UNICEF website, <www.unicef.org/csr/tools.htm>.

The tool features worksheets for six self-assessment areas:

1. **Legal** – Ensuring corporate policies and management processes comply with applicable legislation
2. **Human Rights and Corporate Responsibility** (Human Rights & CR) – Integrating child rights considerations into all appropriate corporate responsibility policies and management processes
3. **Human Resources** – Working to make sure all employees are aware of child rights and exhibit appropriate behaviours
4. **Procurement** – Working with suppliers to align values, expectations and performance
5. **Product Development** – Creating safer and age-appropriate online environments through product development, in use, and through interaction with customers and users
6. **Commercial** – Ensuring marketing, sales, products and services promote child online safety

Each of these areas is related to the department responsible for the key organizational functions of an ICT company, in the areas that are most likely to influence the company’s management of and impact on children’s rights. The aim is to guide users on identifying the parties within their company they may need to engage to complete the assessment, as well as to understand where impacts lie within the company’s value chain.

As appropriate for your business scope and context, the Child Online Safety Assessment can be used at multiple levels, from headquarters to country offices, as well as for subsidiaries.

Value chains and company structures are unique to each business operation, and the tool recognizes that the defined ‘self-assessment areas’ are general categories. Users may therefore find that a function or department is responsible for topics across multiple assessment areas, for example, ‘Legal’ will also be responsible for all or parts of the questions in ‘Human Resources’ and ‘Commercial’.

**Format and structure:** The six worksheets are aligned to business functions as specified above. Each worksheet contains multiple topics; under each topic, specific criteria are listed to assess management of impacts in that area. That is the essence of the tool. An Excel-page snapshot is shown below, with added highlights on the basic steps:
Columns

1–4

<table>
<thead>
<tr>
<th>Topic</th>
<th>Assessment Criteria/Indicator</th>
<th>Result</th>
<th>Status and Evidence</th>
<th>Party Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 CHILD SEXUAL ABUSE MATERIAL (CSAM) POLICIES AND PROCESSES</td>
<td>Policies on user-generated content</td>
<td>Not met</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>1.2 Documented processes for handling CSAM, and escalation when necessary</td>
<td>Assessment criteria/Indicator: The company has approved and implemented handling and escalation processes, beginning with monitoring and extending to the final transfer and destruction of the content.</td>
<td>Partially</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>1.3 CSAM policies and procedures for cooperating with law enforcement</td>
<td>The company works with local law enforcement and other relevant authorities and has agreed processes in place to identify those the company can engage to help address child abuse in the area.</td>
<td>Not met</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>1.4 CSAM policies and procedures for connecting to hotline</td>
<td>The company has developed a working relationship with the national helplines where they exist and has agreed processes for reporting CSAM to them, or is working to ensure a mechanism for reporting CSAM is established if there is none in the country of operation.</td>
<td>Fully</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>

**Assessment Criteria/Indicator** appears in column 2 noting the criteria to ensure that the topic is addressed. These include the presence of existing policies, risk assessments, processes, and procedures as well as their implementation, monitoring, reporting and other proactive measures to address business impacts on child rights.

**Result** – Fully, Partially, Not met, N/A – appears in column 3, via a drop-down menu that is revealed when you click on the bottom-right corner of the cell next to each item.

To answer these questions, read the assessment criteria/indicator for each self-assessment area. Does your company meet the criteria? Are you doing enough to effectively manage this aspect? Assess and answer by clicking on the bottom-right corner of the cell to reveal the drop-down menu. If the question does not apply to your company, choose ‘N/A’ and use the ‘Status and Evidence’ column to record why the item is not related to the company’s operations.

**Status and Evidence** appears in column 4. Use the cells in this column to record what you are currently doing, strengths and weaknesses, as well as any regional and/or product and service variations. For example, developing a code of conduct including child rights/aligned to the Children’s Rights and Business Principles, conducted global risk assessment including issues related to child rights (regional risk assessments under
development).

Also record the names of the documents used as evidence for your assessment here. Keep copies of these documents and records in a secure, easy-to-access corporate archive (e.g., corporate intranet or shared central server). It is recommended that file names align to tool naming/numbering so current and future users can easily locate documentation (e.g., 1.1.1_Policies on user-generated content_Baseline.pdf, 1.1.1_Policies on user-generated content_Further action.pdf). If documentation is accessible via the company website or intranet, include the link in the tool.

Completing these four columns fulfils the core functions of the assessment.

Columns 5 and 6

Allocating ‘Risk’ and ‘Priority’ levels: These two items are optional, though highly desirable in many cases. Conducting a risk analysis as part of the Child Online Safety Assessment will help identify priorities, as well as provide an opportunity to integrate the findings within existing human rights risk assessment and management. If you choose not to assess the risk and priority levels, hide these columns in the tool.

Risk (High, Medium, Low) appears in column 5. Assigning a risk level takes two points of view – impact risk and business risk:

Impact risk considers the likelihood and potential severity of the effects on children, including the scale, or numbers of children who are likely to be affected, and the scope, or importance of the potential effects, for example, impeding access to education, exposure to harmful chemicals/toxins, lack of access to medical care, exposure to sexual/physical violence, possible injury/death or separation from their families.

In many cases, companies do not have as deep of insights into impact risks as they do into business risks. In this case, it is recommended that companies work with stakeholders who are experts in child rights for their industry or sector (e.g. non-governmental organizations, academics) to identify and analyse impact risks. Additional resources are available to help identify and understand the nature of impacts to children in different locations globally, see http://www.childrensrightsatlas.org/.

Business risk considers potential consequences associated with failing to meet the assessment criteria, for example, the financial liabilities if fines are imposed; damage to the company’s reputation; restricted market access and inability to implement a product, service or business model; or limitations due to a business partner’s response when their expectations are not met.

For the purpose of this assessment, business risk should be assessed by the individual or team leading completion of the Excel tool worksheets, during the final stages of the assessment and considering both the self-assessment results in each area and the impact risk for the specific area.
To determine a single risk level, consider likelihood and significance for both the business and impact risk associated with the assessment area/criteria. The risk allocated should assume the highest risk level of the two, for example:

- If either the business risk or impact risk is judged to be potentially high impact, allocate the risk as ‘High’.
- If either the business or impact risk is judged to be medium impact and the other low impact, the overall risk will be ‘Medium’.

**Priority allocation** (High, Medium, Low) appears in column 6. Use this column to assign a priority level to each assessment area that will, in turn, drive actions after the Child Online Safety Assessment is completed. To prioritize actions, first consider the risk assessment outputs – the highest risks should have higher priority for action. Next, consider the company’s progress in this area: Have the criteria been fully addressed, partially addressed, or not addressed at all? Also consider the department/company capacities for taking action to mitigate the risk, and whether control or influence over the assessment area is within the given responsibilities of the business.

1. **Legal – Ensuring corporate policies and management processes comply with applicable legislation**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Assessment Criteria/Indicator</th>
<th>Result</th>
<th>Status and Guidance</th>
<th>Party Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1 Child Sexual Abuse Material (CSAM) Policies and Processes</td>
<td>Risk assessment outputs – the highest risks should have higher priority for action.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.2 Procedures for handling CSAM, and for escalation where necessary</td>
<td>Risk assessment outputs – the highest risks should have higher priority for action.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.3 CSAM policies and procedures for cooperating with law enforcement</td>
<td>Risk assessment outputs – the highest risks should have higher priority for action.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.4 CSAM policies and procedures for reporting</td>
<td>Risk assessment outputs – the highest risks should have higher priority for action.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Column 7**

**Party Responsible** appears in column 7. Recording this information is crucial to engaging the stakeholders who are needed to complete the assessment, and to understanding who will be responsible for future actions related to the assessment criteria/indicator.
Visual and Data Outputs

When the worksheets are filled out, the tool automatically generates charts that summarize the results, documenting the company’s strengths and weaknesses in regard to protecting children’s rights, as well as actions that can be taken to improve alignment with guidelines and best practices.

Click on the ‘Visual Outputs’ tab to view charts on progress across key functions, and progress in addressing baseline expectation and criteria for further action.

![Percentage of criteria met, by self-assessment area](chart.png)
Use the ‘Data Outputs’ tab to view the numbers (raw data) for each chart.
GUIDANCE TABLES FOR THE CHILD ONLINE SAFETY ASSESSMENT TOOL

The Child Online Safety Assessment Tool contains six worksheets for the self-assessment areas:

1. Legal
2. Human Rights and Corporate Responsibility (Human Rights & CR)
3. Human Resources
4. Procurement
5. Product Development

Guidance tables are provided below for each worksheet. These tables are designed to support those conducting the self-assessment on how to interpret the questions and criteria in every area, as well as how to improve the company’s performance against the criteria and address any issues identified in the assessment. The tables outlines the:

• Business department often responsible for the self-assessment area (name of worksheet tab)
• Topics
• Assessment area criteria/indicator
• Risk scenarios associated with poor management in each area
• Guidance on assessing adherence to the criteria (noted as ‘Fully’, ‘Partially’ or ‘Not met’ in the Excel tool) and recommendations for the company’s follow-up actions.

Users are encouraged to refer to these guidance tables prior to and throughout filling in the worksheets to ensure accurate completion and results. As needed, users may also find the guidance tables helpful in providing context and background for stakeholders who are involved with the assessment but may not specialize in such topics.
1. Legal – Ensuring corporate policies and management processes comply with applicable legislation

### 1.1 CHILD SEXUAL ABUSE MATERIAL (CSAM) POLICIES AND PROCESSES

#### 1.1.1 Policies on user-generated content

**Assessment criteria/indicator:** The company has adopted policies regarding ownership of user-generated content, including the option to remove user-created content at the user’s request. The company removes content that violates its child-protections policies and alerts the user who has posted it about the violation.

**Risk scenario:** Users inadvertently or intentionally post child sexual abuse material.

**Guidance/recommendations:** Corporate policies should clearly indicate that a user’s failure to comply with acceptable use will have consequences, including: removal of content, and suspension or closure of their account; revoking a user’s ability to share particular types of content or use certain features; and referring violations to law enforcement.

If the application or service allows customers to upload and store photographs on servers that the company owns or operates, processes and tools are in place to identify images that are most likely to contain child sexual abuse material. Consider proactive identification techniques such as scanning technology or human review.

#### 1.1.2 Documented processes for handling CSAM, and for escalation when necessary

**Assessment criteria/indicator:** The company has approved and implemented handling and escalation processes, beginning with monitoring and extending to the final transfer and destruction of the content.

Roles are clearly identified within the company regarding who is accountable for handling potential child sexual abuse material when it is reported, and for escalation as required. This includes providing details on handing over cases of illegal material to authorities and specifying when the company’s role in an investigation is concluded.

**Risk scenario:** Employees are not clear on how to handle child sexual abuse material and potentially illegal content, leading to responses that are not appropriate or timely. Poor record-keeping or unclear processes for the company’s roles in investigations pose potential legal jeopardies.

**Guidance/recommendations:** Although ICT companies should be able to deal with CSAM and potentially illegal content effectively and in a timely manner, evidence suggests that businesses are not always adequately prepared.

These practices should be clearly defined with assigned focal points, established monitoring and reporting systems, and procedures for transferring evidence to law enforcement when appropriate. Escalation processes must be relevant across all countries of operation and supported by cross-country coordination. While recognizing that laws and enforcement vary in each jurisdiction, the company should publicly commit to dealing with illegal content in the most effective manner, according to national and international legislation, and to working with enforcement agencies.

#### 1.1.3 CSAM policies and procedures for cooperating with law enforcement
### Assessment criteria/indicator:
The company works with local law enforcement and other relevant authorities and has agreed processes in place to identify those using the company’s services to exploit or abuse children.

The company works with internal functions such as customer care, fraud and security to ensure that the business can submit reports of suspected illegal content directly to law enforcement and hotlines. Ideally, the procedure does not expose front-line staff to the content or re-victimize the affected children.

### Risk scenario:
Ineffective or failed responses in case of incidents lead to legal jeopardy or damage to the company’s reputation.

### Guidance/recommendations:
Along with coordinating in-company procedures, building relationships with the relevant law-enforcement agencies will help the business develop uniform procedures for addressing incidents and ensure effective responses.

In jurisdictions that lack adequate legal frameworks and/or governance over the protection of children’s rights, companies should leverage the resources of peers and local/international non-governmental organizations with the aim of implementing consistent procedures – building trust, developing joint solutions and establishing reporting processes that result in the most effective response. Companies should first seek to engage with local agencies and organizations, and where not available, turn to international organizations.

### 1.1.4 CSAM policies and procedures for connecting to CSAM reporting mechanisms/hotlines

### Assessment criteria/indicator:
The company has developed a working relationship with the national hotlines where they exist and has agreed processes for reporting CSAM to them, or is working to ensure a mechanism for reporting CSAM is established if there is none in the country of operation.

### Risk scenario:
Mechanisms to report illegal content are absent or ineffective.

### Guidance/recommendations:
Where they exist, national hotlines or connections to hotlines in a country near by provide the most effective mechanisms for reporting child sexual abuse material.

Company websites should provide links to national hotlines. In places where a hotline has not been established, the site could refer to INHOPE, [www.inhope.org](http://www.inhope.org), which offers reporting links for many countries around the world.

### 1.1.5 CSAM reporting mechanisms/hotlines

### Assessment criteria/indicator:
The company promotes CSAM reporting mechanisms and makes sure that customers know how to make a report if they discover such content. If a national hotline is available, the company offers links to that hotline from its corporate website and from any relevant content services promoted by the company.

If a company is operating in markets with less developed regulatory and law enforcement oversight of this issue, it can refer reporters to the INHOPE Association, [www.inhope.org/gns/home.aspx](http://www.inhope.org/gns/home.aspx), where any of the international hotlines can be selected to make a report.
**Risk scenario:** Because customers and users are not aware of how to report inappropriate content or child sexual abuse material, this content remains available on the Internet.

**Guidance/recommendations:** Operational-level reporting mechanisms should be in place for all countries of operation and accessible based on user demographics, for example, in local languages, stage appropriate, and easy to find and use. National and international hotlines often provide an effective reporting mechanism.

Where a national hotline exists, offer easily accessible links, or offer links to INHOPE to enable international reporting. Customers can also be reminded of this remedy through education on responsible-use mechanisms.

### 1.1.6 Notice and takedown processes

**Assessment criteria/indicator:** The company has processes in place to immediately remove access to child sexual abuse material – including notice and takedown processes and procedures in place to remove CSAM/illegal content as soon as a court or a legitimate administrative authority has ordered such removal or disablement.

**Risk scenario:** Illegal content remains accessible longer than necessary, and opportunities to reduce risks to children are missed.

**Guidance/recommendations:** Consider implementing a simple and highly visible ‘report abuse button’ that takes users through to the reporting mechanism. Put in place an effective filter to sift malicious but non-illegal and potentially illegal content reports, and ensure all reports are swiftly passed through to an enforcement agency or hotline for review. Any decision on illegality should be made by a competent legal authority and be free of political, commercial or other unwarranted influences. Also note the importance of the complaints procedure.


### 1.1.7 CSAM filtering and blocking

**Assessment criteria/indicator:** If the application or service allows customers to upload and store photographs on servers that are owned or operated by the company, have processes and tools in place to identify images that are most likely to contain child sexual abuse material. Consider proactive identification techniques such as scanning technology or human review.
**Risk scenario:** Known illegal content resurfaces, re-exposing the victim.

**Guidance/recommendations:** On a regular basis, actively assess commercial content hosted on the company’s servers, both branded and contracted from third-party content providers. Where possible, create proactive technical measures to block known illegal content, including in private groups, and to analyse the objects and metadata linked to a profile to detect criminal behaviour or patterns – and take the appropriate action.

Many options, such as photo hashing technology, are available for filtering and blocking illegal content. Currently, however, these technologies can be costly to implement and maintain. Working in partnership with others seeking similar solutions is likely to lead to a more effective approach to blocking and filtering, often this may most effectively be achieved at the ISP level.

When limiting access to content in order to protect children, also take care that children and young people are not inappropriately restricted from accessing legitimate and helpful information.

### 1.1.8 Recording and retaining evidence

**Assessment criteria/indicator:** The company documents and securely stores detailed records concerning CSAM, whether images or other formats – and any related activity of concern, e.g., notifications, warnings, penalties/lines, withdrawal of user privileges – so this information can be available for further actions or law enforcement if appropriate. This is done in accordance with local law.

**Risk scenario:** Evidence is not retained and is therefore unavailable to law enforcement agencies.

**Guidance/recommendations:** Effective policies and procedures for documenting and retaining evidence should be established to ensure that all relevant evidence is passed on to law enforcement when legitimate and legal requests are received. This includes records of the profile/location of where it was discovered, and notification of the person(s) responsible for the policy.

### 1.1.9 Non-complicity

**Assessment criteria/indicator:** Strategies are in place to anticipate, respond to and minimize adverse impacts on privacy and freedom of expression where governments are believed to be using the company’s products or services for illegitimate or political purposes, e.g., requesting service restrictions or requesting non-legitimate information about individuals.

**Risk scenario:** The company becomes complicit in human and child rights violations by governments or others in the context of freedom of expression, the right to privacy, or other rights.

**Guidance/recommendations:** Carefully evaluate the legitimacy of government requests for users’ information. This can include: ensuring that governments follow established domestic and international legal processes and standards related to any requests; confirming the legal basis and the specific nature of the request in writing from an authorised signatory of the government department making the request; interpreting the request in light of the above to minimise any negative effects on freedom of expression; being prepared to challenge the requests if they appear not to have a sound legal basis, are overbroad or inconsistent with standards in this area.

Further information can be found from the Global Network Initiative [https://globalnetworkinitiative.org/principles/index.php](https://globalnetworkinitiative.org/principles/index.php)
### 1.1.10 Terms and conditions covering CSAM

**Assessment criteria/indicator:** Terms and conditions specifically prohibit using mobile services to store, share or distribute child sexual abuse materials.

These terms clearly state that illegal content, including child sexual abuse material, will not be tolerated, and that the company will collaborate fully with law enforcement investigations in the event that illegal content is reported or discovered.

**Risk scenario:** The company fails to communicate unacceptable use of products and services, and contractual provisions regarding illegal behaviour.

**Guidance/recommendations:** Terms and conditions of service should explicitly prohibit illegal content and behaviour, highlighting the following items:

- Illegal content, including child sexual abuse material, will not be tolerated.
- The company will cooperate fully with law enforcement investigations in the event that illegal content is reported or discovered.
- The company is committed to international human rights standards and law, and will not unnecessarily prohibit the free flow of information on the Internet.

### 1.1.11 Finance trail

**Assessment criteria/indicator:** The company takes steps to prevent the misuse of its payment services (mobile or otherwise) to monetize child sexual abuse content.

**Risk scenario:** Payment services are used to monetize child sexual abuse material.

**Guidance/recommendations:** Following financial flows may be an effective way to identify perpetrators of crimes against children, and can provide significant evidence that enables successful prosecutions.

The company interrogates and uses its own payment and financial systems to provide evidence to appropriate authorities regarding monetizing child sexual abuse material.

See the European Financial Coalition for more information [http://www.europeanfinancialcoalition.eu/](http://www.europeanfinancialcoalition.eu/)
2. Human Rights and Corporate Responsibility (Human Rights & CR) – Integrating child rights considerations into all appropriate corporate policies and management processes

### 2.1 CHILD SAFEGUARDING POLICIES AND PROCESSES

#### 2.1.1 Accountability

**Assessment criteria/indicator:** A specific individual or team is designated with the responsibility for managing the company’s child online safety performance. The company provides this person or team with access to the necessary internal and external stakeholders, and gives them the authority to raise the profile of children’s rights online across the business operations.

**Risk scenario:** Insufficient leadership and support, lack of accountability and weak governance, leading to ineffective management response to the issues and potential damage to the company’s reputation.

**Guidance/recommendations:** Assign an individual or team with accountability and clearly define their responsibilities. ICT companies can prioritize the material aspects of children’s rights, based on their business model, products and services. A board-level sponsor can be appointed to hold final accountability. The individual or team designated with responsibility needs access and support to implement risk prevention and mitigation actions.

#### 2.1.2 Child safeguarding policy

**Assessment criteria/indicator:** The company has made a clear public commitment to child online protection, safeguarding and promoting children’s rights across all countries of operation.

A policy exists and/or specific children’s rights risks and opportunities have been integrated into companywide policy commitments, such as human rights, privacy and marketing policies and relevant codes of conduct.

At minimum, the child safeguarding policy covers the commitment to meet international and regional standards in regard to:

- Integrating child rights considerations into all appropriate corporate policies and management processes.
- Creating a safer and age-appropriate online environment.
- Collaborating with law enforcement investigations in the event illegal content is discovered, and developing standard processes to handle child sexual abuse material.
- Educating children, parents and teachers about children’s safety and their responsible use of information and communication technologies.
- Promoting digital technology as a mode for increasing civic engagement and advancing human rights.
**Risk scenario:** Unclear definition of the company’s position on children’s rights results in heightened risk of rights violations. Additionally, a lack of public commitment is a reputational risk.

**Guidance/recommendations:** Although there is no linear process for integrating children’s rights into a company’s policy framework, the following points can be considered:


- Prioritize material issues that present the greatest areas of risk and opportunity for impacting children’s rights. Involve internal and external stakeholders in the process, and work with suppliers, customers and business partners to identify their potential risks to children’s rights that might differ from the company’s direct operations.

- Map existing policies and codes of conduct to identify coverage of priority children’s rights issues for the company and where there are gaps – for example, policies and codes of conduct relating to human rights, health and safety, privacy, marketing, suppliers, procurement and ethics. Also consider coverage in terms of business relationships such as supplier contracts.

- Obtain senior-level commitment, assign senior management responsibility, and allocate responsibilities and resources for addressing issues related to children to relevant functions within the business.

- Ensure effectiveness by embedding children’s rights policies within the company’s procedures and culture. This could be carried out through training, leadership incentives and accountability structures.


### 2.1.3 Policy for broadcasting

**Assessment criteria/indicator:** The company has developed policies that safeguard the physical and emotional welfare and dignity of people under 18 who are involved in or contribute to broadcast content, e.g., for use in television content that is also used online.

**Risk scenario:** Broadcasters and producers impinge on children’s rights within the programme production value chain.

**Guidance/recommendations:** Licensing agreements for producing content for broadcast or online interaction should include child protection measures, irrespective of consent that might have been given by a parent or other adult guardian. The company should ensure that child safeguarding procedures cover both production and distribution, e.g., for online platforms.

### 2.1.4 Child rights impact assessment

**Assessment criteria/indicator:** The company has assessed child rights impacts and the risks to children from its business model, in the context of its operating countries or regions and from a product and technology perspective.
**Risk scenario:** Potential violations against children’s rights are not understood across all of the company’s operating environments.

**Guidance/recommendations:** All child rights assessments should identify potential and actual risks in the delivery of products and services throughout the value chain. Engaging with regional and local stakeholders, can help inform specific risks in countries of operation, including when entering new markets.

Additionally, companies can consider how the products and services are actually used, and whether children are using products and services that were intended for adults.

Additional resources are available to help identify and understand the nature of impacts to children in different locations globally, see [http://www.childrensrightsatlas.org/](http://www.childrensrightsatlas.org/).

### 2.1.5 Business risk

**Assessment criteria/indicator:** The company has conducted a thorough child rights risk assessment, using the Child Online Safety Assessment or other authoritative tool for guidance, and understands the implications of its impacts on children’s rights in relationship to its operations.

**Risk scenario:** Potential impacts on children – and the significance and consequences of these impacts – are not clearly understood at the corporate level, leading to infringements of child rights. Resources are not sufficiently focused on areas where the company can make the most significant difference.

**Guidance/recommendations:** ICT companies should seek to understand the specific impacts associated with their business activities. Assessing overall risks at the corporate level should cover all functions that impact on children throughout the value chain, from sourcing to end of product or service life.

Examples of potential impacts include but are not limited to: making and sharing child sexual abuse material, grooming, cyberbullying, trolling, negative influence on perceptions of body and self-image, violations of privacy and data protection, negative financial impacts on customer due to child use of services.

Incorporate child rights criteria into existing human rights or other policies where relevant.

### 2.1.6 Internal stakeholder consultation

**Assessment criteria/indicator:** Key internal stakeholders have been consulted on child online safety mechanisms to highlight the company’s policies and to obtain ongoing feedback and guidance on its approaches to ensure that they are effective.

**Risk scenario:** Messages and mechanisms within the organization are inconsistent; learning opportunities are missed.

**Guidance/recommendations:** Drawing on experience from relevant roles across the business can help identify optimal solutions and approaches to promoting children’s safety online. It is important that sufficient regional and in-country stakeholders are included to represent high-value and high-risk regions, as well as the diversity of locations where the company operates. This can be supported by mapping the internal stakeholders who are relevant and necessary to evaluating child online safety mechanisms, according to both their function and location.

### 2.1.7 External stakeholder consultation

**Assessment criteria/indicator:** Key external stakeholders, including children and experts, have been consulted on child online safety mechanisms to obtain ongoing feedback and guidance on company approaches to ensure they are effective.
Risk scenario: Failure to evaluate child online safety mechanisms objectively; missing external viewpoints and thus opportunities for improving mechanisms and methods.

Guidance/recommendations: External stakeholders who understand the issues and potential solutions can be found among international organizations and agencies, non-governmental organizations or community investment project partners; suppliers, industry associations and trade unions; and recruitment agencies or providers for outsourcing services.

During stakeholder consultation on issues that affect children, it might be sufficient to consult with their representatives such as parents, caregivers, local organizations, and the country or regional offices of international agencies.

In cases when it is necessary and appropriate to consult directly with children, such as identifying how they actually use products and services, be sure to follow the established standards. Guidance on working with children is offered, for example, in UNICEF’s Engaging Stakeholders on Children’s Rights, ‘Part III: How to consult children directly’. This tool for companies is available at: <www.unicef.org/csr/engagement.htm>.

2.1.8 Network for implementing child safeguarding policies

Assessment criteria/indicator: All business functions – including compliance, product development, social media and online safety – coordinate their activities to ensure that policies for safeguarding children are fully incorporated and implemented in all types of user interactions with children and other customers.

Risk scenario: Ineffective and inconsistent response to reported incidents or concerns.

Guidance/recommendations: A coordinated response can minimize established risks to children’s rights and ensure that learning is shared across business operations in a timely manner. Where effective processes have been developed in one part of a company, consider how these may apply to other business units, group companies and regions. Coordination can also confirm that appropriate resources are allocated in areas where the company can make the most difference. Additionally, exposure to child sexual abuse material and other child safety and well-being issues can negatively impact effected employees, who benefit from a support network.

2.1.9 Internal and external monitoring and evaluation

Assessment criteria/indicator: Internally, the company has identified appropriate performance indicators to track progress/monitor performance in areas of high risk for children's rights.

At least once a year, external monitoring and evaluation is conducted by a suitable governance body to assess the company’s performance and progress regarding children’s rights. The results of this external review, as well as expected internal changes in response to the outcome, are clearly communicated to the company.

Risk scenario: Inadequate indicators for measuring the effectiveness of the company’s processes and approaches and/or insufficient external oversight can lead to missed opportunities to improve performance regarding child rights.

Guidance/recommendations: Understanding the key areas the company can influence is a good first step, followed by introducing performance indicators for monitoring progress in these areas. Targets can then be used to help drive improvements. Building in an annual review by an appropriate governance forum provides an opportunity to confirm the effectiveness of the business approach to addressing online safety.

Potential indicators could include: percentage of child distress messages responded to within 24 hours, absolute numbers of children’s rights infringements by region. These can also be normalised by comparing to another established business metric, such as revenue or numbers of service users.

A key resource for developing child rights risk indicators is the Children’s Rights and Business Atlas, <www.childrensrightsatlas.org>, an interactive data-driven platform, jointly produced by UNICEF and the Global Child Forum. Through global interactive maps and country scorecards, the atlas enables quantitative evaluation of the degree to which children’s rights are protected within 198 countries and territories, across
2.1.10 Corporate reporting

**Assessment criteria/indicator:** The company internally and publicly reports on its performance in areas of child rights-related impacts, risks, and initiatives to mitigate and manage the risks.

**Risk scenario:** Lack of transparency impacts business credibility, for example, when issues are revealed in the public domain through other channels, placing the business at greater risk.

**Guidance/recommendations:** Transparency is key to working in partnership to tackle and reduce a company’s potential and actual negative child rights impacts and promote its positive impacts on children. Good practice also includes, for example, public reporting of numbers of grievances raised, investigated and resolved and the time frame to conclude.

2.1.11 Grievance reporting mechanisms (general, plus criteria for broadcasting)

**Assessment criteria/indicator:** Grievance and reporting mechanisms for any potential and actual child rights violations – including but not limited to child sexual abuse material, content or contact that is not age appropriate, and privacy breaches – are in place and accessible for all stakeholders, including in all local languages in operating countries. These mechanisms are promoted to parents and users.

*In regard to broadcasting, the production company and/or broadcaster has an appropriate mechanism in place for reporting concerns and suspected abuse when children are involved in pre-production and production.*

**Risk scenario:** Customers/users cannot find or use reporting and grievance mechanisms, e.g., for child sexual abuse material, inappropriate content or contact, breaches of privacy and bullying. Broadcasters do not have appropriate reporting processes in place during production or at the time of broadcast.

**Guidance/recommendations:** Ensure appropriate reporting mechanisms are promoted with access routes from each game, product or service, and that they are accessible and easy to understand and use.

Refer any incident of suspected grooming promptly to the online or interactive executive management team that is responsible for reporting it to the appropriate authorities:

- Make sure that a team member is available by phone when online interactive services are aimed to a young audience; this phone number should also be accessible via a broadcaster’s switchboard.
- Establish common email addresses linked to the function (not the names) of team members to automatically alert those on duty of incidents.
- When a content producer refers a report of suspected grooming to the interactive executive management team, she or he should also report it to the nominated child protection policy manager.
- Make it possible for users of a broadcaster’s site to report suspected grooming incidents directly to authorities.

2.1.12 Communicating remediation outcomes

**Assessment criteria/indicator:** The outcomes of any complaint, grievance or violation, including any corrective actions taken, are communicated back to internal and external stakeholders as appropriate.
**Risk scenario:** Impacted individuals are not informed of the outcome.

**Guidance/recommendations:** A process defining who is responsible and how to respond to raised concerns should be in place, and those involved in processing complaints, grievances or violations should participate in training on how to close incidents appropriately. When grievances are passed to external parties and the company’s involvement is completed, this is communicated to parents and other external parties as appropriate.

### 2.2 CORPORATE SOCIAL RESPONSIBILITY

#### 2.2.1 ICT for development

**Assessment criteria/indicator:** The company aligns with existing national government development plans to use ICT for development and to bridge the digital divide, with a focus on children.

**Risk scenario:** Missing an opportunity to enable ICT to have positive development impacts aligned to an overall strategy or plan.

**Guidance/recommendations:** The digital divide refers to the gap between those who have access to ICT’s and those who don’t or have limited or poor quality access. Ensure good working relations with government, international agencies and other stakeholders involved in national development plans. This can help ensure alignment with legitimate policy objectives and priorities and can help multiple up available funds and other resources to implement these policies.

#### 2.2.2 Educational programmes

**Assessment criteria/indicator:** If the business already works with children or schools, for example, through corporate social responsibility programmes, the company has investigated whether this can be extended to include educating children and teachers on safe Internet use.

**Risk scenario:** Opportunities to leverage existing resources in support of online safety programmes and initiatives are missed.

**Guidance/recommendations:** External programmes to promote online safety and protection of child rights will often align with the company’s social responsibility priorities and/or existing initiatives. Leveraging existing programmes and stakeholder relationships can, for example, support the implementation of educational programmes with fewer resources, while expanding the impact of the company’s social initiatives.

#### 2.2.3 Access to ICT

**Assessment criteria/indicator:** The company considers children and young people who are marginalized, living in poverty or residing in underdeveloped areas as a consumer segment at the country level. It works to ensure access to information and communication technologies for underprivileged and vulnerable children and schools, including those located in remote areas.

**Risk scenario:** Missed commercial and social value opportunity, as well as the opportunity to link corporate philanthropy to children and young people.

**Guidance/recommendations:** Based on a country or region’s development needs and the situation of the poorest people, product and service delivery can support mechanisms for advancing child rights and broader social benefits. Look for opportunities to leverage corporate philanthropic programmes to support and expand efforts to serve poor or marginalized populations.
### 3. Human Resources – Working to make sure all employees are aware of child rights and exhibit appropriate behaviours

#### 3.1 DUE DILIGENCE

##### 3.1.1 Recruitment

**Assessment criteria/indicator:** The company checks potential new staff, contractors and collaborators who work with children to confirm that they are not a risk to children, including criminal record checks if appropriate. Background checks are also conducted for anyone moderating a public electronic interactive service that is likely to be used by children.

**Risk scenario:** Known paedophiles or individuals with known risk profiles are employed in roles that include contact with children.

**Guidance/recommendations:** These roles, including market researchers, and chat room and other social media platform moderators, require preliminary background and criminal record checks with law enforcement authorities.

##### 3.1.2 Employee training and learning

**Assessment criteria/indicator:** All employees in roles that involve interaction with or protection of children – including in the design, development or moderation of products and services – have participated in targeted training on child safety. This training includes guidance on protecting children’s privacy, how to deal with bullying, understanding youth issues, and identifying and addressing children’s risks in regard to grooming for sexual purposes.

**Risk scenario:** Unsafe or inappropriate behaviours related to the company’s products and services through the value chain cause child rights violations; the quality and approach to interaction with children online varies across the company’s products and services.

**Guidance/recommendations:** ICT companies have the opportunity to address these risks by ensuring that all individuals and teams that interact directly with children or indirectly through children’s use of products and services participate in training. This includes education on the risks, potential and actual impacts, and ways to avoid and mitigate impacts.

Product and service developers have a key role in designing in child safety and therefore their training requirements should help enable this to happen. Training can be provided for front-line staff and child-safeguarding teams to cover prevention of unsafe behaviours and suitable responses – and to handle different types of incidents in order to ensure that responses are sufficient and appropriate actions are taken. Additional training and availability of support to maintain good mental health when dealing with cases of child sexual abuse and exploitation can benefit staff well-being.

##### 3.1.3 Record-keeping on training

**Assessment criteria/indicator:** Relevant employee training is documented, including the names and roles of people who attend training, dates, format/length, numbers attending each course or module, and any score, certification or confirmation of successful completion.
**Risk scenario:** Company is unable to effectively track which employees have fulfilled training requirements, leaving open the risks of child rights violations or failure to respond effectively to incidents involving children.

**Guidance/recommendations:** Consider integrating a tracking system specifically for child rights education within existing corporate-level data management to track training.

### 3.1.4 Code of conduct provisions

**Assessment criteria/indicator:** *The company’s code of conduct for employees includes provisions that explicitly forbid accessing child sexual abuse material and other illegal behaviour.*

**Risk scenario:** Internal standards to address potential risks of child rights violations are not clearly established or communicated.

**Guidance/recommendations:** Use codes of employee conduct to prohibit illegal content and behaviour, highlighting that:

- Illegal content, including child sexual abuse material, will not be tolerated.
- The company will cooperate fully with law enforcement investigations in the event that illegal content is reported or discovered.
- The company is committed to international human rights standards, and law and will not unnecessarily prohibit the free flow of information on the Internet.

### 3.1.5 Employee protection

**Assessment criteria/indicator:** *The company has established a process for handling abusive/illegal content that, ideally, protects front-line staff from exposure to child sexual abuse material. If staff are exposed to CSAM, a programme is in place to support staff resilience, safety and well-being.*

**Risk scenario:** Employees are exposed to child sexual abuse material, raising well-being and legal risks to those employees.

**Guidance/recommendations:** Appropriate processes are in place to avoid re-exposure of flagged child sexual abuse material, such as copying the link only to the content and not to the content itself. Support services can include telephone or in person counselling, a support network of other colleagues involved in aspects of children's rights management, and appropriately trained line managers.
### 4. Procurement – Working with suppliers to align values, expectations and performance

#### 4.1 DUE DILIGENCE

**4.1.1 Supplier contracts**

**Assessment criteria/indicator:** All contracts with suppliers throughout the value chain incorporate the same requirements and standards for safeguarding children as the company’s policies and codes of conduct.

**Risk scenario:** Potential violations of children’s rights in the company’s value chain.

**Guidance/recommendations:** Actions of suppliers are increasingly leading to risks to established brands. It is essential that similar standards are driven across the value chain, both upstream and downstream to all suppliers involved in the development or delivery of products and services. Contracts and engagement with suppliers should draw on existing policies, codes of conduct and approaches to support the supplier in developing and implementing child safeguarding standards if they are currently absent or insufficient.

**4.1.2 Supplier selection**

**Assessment criteria/indicator:** The company has assessed child rights impacts and risks in relation to third-party suppliers and throughout the value chain.

**Risk scenario:** Limiting assessments to directly controlled operations can miss significant risks.

**Guidance/recommendations:** Partnering with suppliers and other business relationships can help to identify and manage potential and actual impacts on children’s rights. Use a systematic approach to assessing third-party risks as part of the supplier contracting due diligence process. Track any infringements by the supplier and include this information in formal supplier performance reviews. Work with suppliers cooperatively to develop plans that will enable timely implementation if child rights violations are reported or discovered, including remediation as appropriate. When minor non-compliance is found, a discussion between the company and the supplier should be initiated to identify and agree on the areas for remediation. If there are major or repeated violations, specific improvement plans with clear timescales should be jointly agreed and implemented. If these plans are not fulfilled, the ultimate sanction is to deselect the supplier.

**4.1.3 Training for suppliers**

**Assessment criteria/indicator:** All third parties contracted by the company in roles that involve interaction with or protection of children – including in the design, development or moderation of products and services – have participated in targeted training on child safety. This training includes guidance on protecting children’s privacy, how to deal with bullying, understanding youth issues, and identifying and addressing children’s risks in regard to grooming for sexual purposes.

**Risk scenario:** Missing the opportunity to design out potentially unsafe behaviours or acts in the development or delivery of company products and services. **Guidance/recommendations:** The company typically has control over the supplier relationship and as such has an opportunity to clarify expectations and to ensure that supplier staff working on the supply of products or services to a company are adequately trained on child right’s infringement risks and appropriate responses. Training can be provided to any staff working on behalf of the company contract to cover prevention of unsafe behaviours and to detail suitable responses.
5. **Product Development** – Creating safer and age-appropriate online environments through product development, in use, and through interaction with customers and users

### 5.1 CUSTOMER AND USER INTERACTION AND EDUCATION

#### 5.1.1 Product and services development

**Assessment criteria/indicator:** The company has assessed if there are opportunities to make a positive impact on children’s rights across different age groups/development stages in the design, development and introduction of new products and services.

**Risk scenario:** Missed opportunities to design in child safety features and measures that promote child right’s.

**Guidance/recommendations:** It is much more effective to build child safety features into ICT’s than to try to deal with the consequences of infringements of rights and the impacts on children. There is a significant opportunity to support age and stage appropriate childhood development through products and services that build in the promotion of child right’s.

For example, online platforms can promote children’s right to express themselves, to facilitate participation in public life and to encourage collaboration and entrepreneurship. These features should be highlighted in information to parents to enable them to better understand some of the benefits use of ICT’s can bring. These features can be used as an opportunity to stimulate innovation and new product and service developments that meet the characteristics of different development stages.

#### 5.1.2 Education, incentives, and using core game characters to promote safety

**Assessment criteria/indicator:** The company offers various forms of education to promote children’s safety and appropriate online behaviours. This includes:

- Providing age-appropriate tools such as tutorials and help centres, and working with online/in-person prevention programmes and counselling clinics in order to deal with identified problems, as appropriate.
- Offering incentives – such as game currencies, credits, or access to new areas/levels or services – to complete online safety training/tutorials and to encourage the right behaviours.
- Using the key characters and features from games to reinforce online safety messages and encourage safe and appropriate behaviours.

**Risk scenario:** Missing opportunities to engage external stakeholders to understand and mitigate risks against children. Lack of resources to deal with potential issues impacting children or causing harm to children, for example, unintended use of products, accessing inappropriate material and bullying.

**Guidance/recommendations:** Utilize key strength of the products and services, such as prominent game characters, to more effectively engage and educate children about online safety. Offering game incentives can also be a useful mechanism to encourage learning about and adoption of safe online behaviours.

#### 5.1.3 Involving parents and adult caregivers
**Assessment criteria/indicator:** The company actively supports the primary role of parents in evaluating and minimizing risks of harm to their children. The company encourages adults, including parents and teachers, to be involved in children’s consumption and use of online content, so that they can assist and guide children in the choice of content when they are making a purchase, as well as helping establish rules of behaviour and good conduct.

**Risk scenario:** Opportunities to raise parents’ awareness on safe online child behaviours are missed.

**Guidance/recommendations:** The responsibility for and opportunity to encourage safe behaviours should be shared across stakeholders. Parents and those closest to the child have the greatest opportunity to influence safe behaviours and the provision of information on how to do this can be targeted at them.

### 5.1.4 Parental controls

**Assessment criteria/indicator:** Simple and intuitive tools/toggles for parental control options are built into products, services and game platforms aimed to children under age 13 to encourage parental involvement and to minimize risk of ‘option setting fatigue’ that can result in low parental involvement.

**Risk scenario:** It is more difficult to prevent unsafe behaviours if control options for parents are not easy to use and relevant for children’s developmental stages.

**Guidance/recommendations:** Building simple and intuitive tools/toggles for parental control options into product services and game platforms aimed for children under age 13 will minimize the risk of ‘option fatigue’ when there are too many or too complicated choices for settings – and encourage parents to be more involved in their children’s online usage.

Set these tools up so they are readily available and clearly state what the controls cover, as appropriate, e.g., while on network, or do not cover, e.g., when on Wi-Fi. Options include lists of safe vs. unsafe web pages (‘white’ and ‘black’ lists, content filters, usage monitoring, contact management, and time/programme limits.

### 5.1.5 Parent portal/advice hub

**Assessment criteria/indicator:** An advice/guidance hub has been created and populated to help users and parents understand the actions they can take to keep safe online.

**Risk scenario:** Missing an opportunity to build trust and brand preference with users.

**Guidance/recommendations:** Transparent, clear and easy-to-use information can help empower young users and the parents or other caregivers.

ICT companies can create a section dedicated to safety tips, articles, tutorials, features and dialogue about digital citizenship, as well as links to useful content from third-party experts and access to help desks or other support services. Safety advice should be easily spotted and provided in clear and simple language.

### 5.1.6 Helplines for children

**Assessment criteria/indicator:** The company promotes national helplines and other services that enable children to seek support in the case of concerns, abuse or exploitation.
**Risk scenario:** Adequate or suitable support options for online issues do not exist.

**Guidance/recommendations:** Companies should seek to ensure that a national helpline exists and support the creation of one where absent in the country of operation. See, for example, Child Helpline International, <www.childhelplineinternational.org>.

### 5.1.7 Monitoring obsessive ICT use

**Assessment criteria/indicator:** Where the company monitors gaming hours and collects statistics on the use of products and services, opportunities are taken to better understand gaming addiction behaviour and to develop responses to users who have obsessive risk profiles.

**Risk scenario:** Users get drawn into games, products and services in an obsessive way that negatively impacts their behaviour and well-being.

**Guidance/recommendations:** The company sets up ways to identify and act on indications of obsessive use. Options for addressing this issue include providing tutorials and other information to help educate users and caregivers, and promoting counselling and helplines that offer support.

## 5.2 CONTENT

### 5.2.1 Child rights impact assessment

**Assessment criteria/indicator:** The company has assessed the child rights impacts and risks on different age groups as a result of the design, development and introduction of products and services.

**Risk scenario:** Missing impacts and risks associated with children’s age and stages of development.

**Guidance/recommendations:** Products and services may include elements that are of lower or no risk to older age groups, but pose risks to younger users. Different age groups have different needs online. There may be a legal requirement, e.g., the US COPPA Act in relation to sharing of personal information relating to children under 13, and varying national legislation regarding requirements for other age groups. Further information about compliance with COPPA can be found at [https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions](https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions).

### 5.2.2 Positive content, appropriate by children’s age and developmental stage

**Assessment criteria/indicator:** The company ensures that age-appropriate content contributes to children’s physical, mental and social development by providing new opportunities for creativity and play at different developmental stages, as well as contributing to learning about the environmental challenges and social issues faced by society.
**Risk scenario:** Children are exposed to harmful content; the company misses an opportunity to build trust and brand preference with users.

**Guidance/recommendations:** ICT products and services offer great new opportunities to learn and to enhance children’s experiences.

Companies can use models such as shared value to consider ways their products and services can be developed and used for social as well as commercial benefit.

Issues such as positive body image, cultural diversity, environmental sustainability, as well as how to deal with and handle bullying behaviours, to protect personal data, to learn how to spot and mitigate online safety risks, are all examples of positive content.

### 5.2.3 Age verification

**Assessment criteria/indicator:** The company sets up appropriate sign-on processes to determine whether users are old enough to access the content or service, and uses nationally established age-verification systems linked to a reporting function or a help desk/centre that can encourage users to report people who have falsified their ages. In addition:

- The company takes steps to identify and remove underage users who have misrepresented their age to gain access.
- A personal identification number (PIN), password or other controlled-access mechanism is required to access content targeted to adults that is inappropriate for children under 18.

**Risk scenario:** Underage users access inappropriate products or services, and parents, guardians or teachers do not realize that children may be accessing stage-inappropriate content. Undetected sharing of personal information by children under age 13 can lead to sanctions, fines, loss of ‘Safe Harbor’ certification, and loss of consumer trust. US-EU Safe Harbor is a streamlined process for US companies to comply with the EU Directive 95/46/EC on the protection of personal data. Certification is a mechanism to demonstrate compliance with the process provisions.

**Guidance/recommendations:** Verifying a user’s age can be a significant challenge; even when mechanisms are in place to verify age, none is infallible. Though contracts for services are typically established by adults, children are using their devices and may be accessing services or content not intended for under 13s. Many users will knowingly report their age incorrectly, typically to get fuller access to product or service features.

To address this issue, ICT companies can: enforce minimum age requirements; take steps to identify and remove underage users who have misrepresented their age to gain access; and support the research and development of new age-verification systems such as biometrics, using international standards for the development of such tools.

Various measures can be used to control access to user-generated content and protect children online against inappropriate or illegal content. Make sure that secure passwords are used as a step towards protecting children in gaming and other social media settings. If they are not already in place, set up appropriate sign-on processes to determine whether users are old enough to access the content or service, and use nationally established age-verification systems linked to a reporting function or a help desk/centre that can encourage users to report people who have falsified their ages.

### 5.2.4 Gateways to other applications
### 5.3 CONTACT

#### 5.3.1 Online chat moderation

**Assessment criteria/indicator:** The company has mechanisms in place to moderate chat-related content to ensure a safe online environment. This includes protecting younger users from uninvited communication.

**Risk scenario:** Chat functions and post-moderated chat environments are used to abuse or exploit children. Users quickly learn the technical limitations of back-end filtering and bypass restrictions on inappropriate or illegal content.

**Guidance/recommendations:** Chat functions should include end-user tools to block, delete, ‘unfriend’ and report abusive comments or an exploitative user. Moderators should receive sufficient training; post-moderation comments require effective filtering and end-user reporting to create a safer online environment.

To minimize ‘false-positive’ reports, screening systems for end-user reports of inappropriate or illegal behaviour or content can be built into the moderation queue.

#### 5.3.2 Image sharing

**Assessment criteria/indicator:** The company has developed and implemented ways to review images before hosting.

**Risk scenario:** Illegal and inappropriate content appears online.

**Guidance/recommendations:** Find ways to review hosted images and videos, and delete inappropriate ones when found. Tools such as hash scanning of known images and image recognition software are available to assist with this. Photos and videos can be pre-checked to make sure that children do not publish sensitive personal information about themselves or others.

#### 5.3.3 Sharing and discussion groups

**Assessment criteria/indicator:** The company has mechanisms in place to review content prior to uploading.
**Risk scenario:** Illegal and inappropriate content appears online.

**Guidance/recommendations:** The company can develop tools that actively seek and remove content that is illegal/in breach of the company’s terms of condition and service, as well as tools to prevent uploading of known illegal content to the site. Discussion groups can be reviewed to find harmful subject matter, hate speech and illegal behaviour, and such content deleted when it is found to violate the terms of use.

### 5.3.4 Message boards

**Assessment criteria/indicator:** The company pre-moderates message boards with a team of specialized children’s moderators who screen for content that violates the published community guidelines, acceptable use policy and/or ‘house rules’.

**Risk scenario:** Illegal and inappropriate content appears online.

**Guidance/recommendations:** Each message can be checked before it is published, and moderators will also spot and flag suspicious users, as well as users in distress;

### 5.3.5 Like-dislike/voting features

**Assessment criteria/indicator:** The inclusion of features for ‘liking-disliking’ or voting on content is carefully considered regarding whether the function is necessary and appropriate, especially for platforms that aim to reach children under 13.

**Risk scenario:** ‘Dislike’ functions can encourage inappropriate behaviour.

**Guidance/recommendations:** Ensure like/vote functionality cannot be used in a way that supports online bullying or trolling. Appropriate training of moderators and pre-moderation are ways to avoid and reduce this risk.

### 5.3.6 ‘Friend’ lists, administration and limiting high-risk profiles

**Assessment criteria/indicator:** The company has mechanisms in place to protect ‘friend’ lists for children under age 13 – including a time delay before accepting the request, allowing parents to make final approvals for incoming requests. In addition:

- Simple and intuitive friend-list administration tools are easily accessible to the user.
- The company limits the ability of users with profiles that have been identified as high risk, e.g., by previous significant or persistent violations of terms and conditions or other legitimate reasons, to become friends.

**Risk scenario:** Paedophiles and other malicious users bypass parental controls, and high-risk profiles are allowed to seek and accept ‘friends’. Children and parents are unable to act when concerns arise.

**Guidance/recommendations:** Empower parents to administer the children’s accounts and actions by providing easy to use parental controls and advice hubs. Consider adopting and monitoring ‘triggers’ that indicate that the ‘friend’ function should be disabled for certain high risk profiles.
## 5.4 CONDUCT

### 5.4.1 Community guidelines

**Assessment criteria/indicator:** The company has developed community guidelines, an acceptable use policy and/or house rules for appropriate use of interactive services, and details the consequences of not following them. They are clearly communicated in user stage-appropriate language, for example, with safety pop-ups that remind users of appropriate and safe behaviour such as not giving out their contact details.

**Risk scenario:** Users are unclear on the boundaries of what is acceptable online behaviour, so mistakenly violate house rules.

**Guidance/recommendations:** Establish, make available and implement clear rules for online conduct. Community guidance can be developed at various intervention points in products and services to make the information ‘bite sized’ and easy to understand at the point of risk.

‘House rules’ are a simplified version of the more detailed terms and conditions or user contract at a game, product or service access level. Setting out the consequences of not following the rules – such as loss of privileges, and game points, or account closures – is also important to encourage responsible behaviour.

### 5.4.2 Self-regulation

**Assessment criteria/indicator:** The company has established and encourages a user ‘trust and reputation’-based system to encourage good behaviour and enable peers to teach best practices to each other by example.

**Risk scenario:** Opportunities for social networking to self-regulate as far as possible are missed.

**Guidance/recommendations:** Promote the importance of social reporting, which allows people to reach out to other users or trusted friends to help resolve a conflict or open a conversation about troubling content. Moderators can help to seed discussions about content which is close to or just crosses the boundaries between acceptable and unacceptable content. They can provide guidance as to how to stay within the user guidelines and can provide specific feedback to individual users privately to help them understand the boundaries of acceptability. Super-users with reputations within the product and service environment may be encouraged to support appropriate use or asked about what they would do in the circumstances.
6. Commercial – Ensuring marketing, sales and products and services promote child online safety

### 6.1 DATA PROTECTION AND PRIVACY

#### 6.1.1 Service transparency

**Assessment criteria/indicator:** *Information provided by the company provides clear details for customers about the nature of the services that are offered, for example:*

- type of content/service and costs;
- minimum age required for access;
- availability of parental controls, including what the controls cover (e.g., network) or do not cover (e.g., Wi-Fi) and guidance on how to use the controls;
- type of user information that is collected and how it is used.

**Risk scenario:** Parents are unable to restrict access or do not know how to report inappropriate or illegal content.

**Guidance/recommendations:** Develop and implement transparent and easy-to-use mechanisms for parental controls and reporting. Explain, for example, the functions of social networking sites and location-based services; how the Internet is accessed via mobile devices; and the options available for parents to apply controls.

#### 6.1.2 Compliance and certification, including verifiable parental consent (VPC)

**Assessment criteria/indicator:** *Where personally identifying information (PII) from children under 13 is collected, used or disclosed, the company complies with the requirements of the Children’s Online Privacy Protection Rule (COPPA) or equivalent.*
**Risk scenario:** If VPC is not implemented, someone who is not a parent or guardian can activate an account for a person under age 13 for the purposes of grooming, viewing this as an incentive for the child to establish or strengthen the link to this adult. Undetected sharing of personal information by children under age 13 can lead to sanctions, fines, loss of Safe Harbor certification and loss of consumer trust.

**Guidance/recommendations:** Requirements under the COPPA legislation regarding companies that collect, use or disclose personal information from children under 13 include:

- Post a clear and comprehensive online privacy policy describing the company’s practices for personal information collected online from children.
- Provide direct notice to parents and obtain VPC, with limited exceptions, before collecting personal information online from children.
- Give parents the choice of consenting to the company’s collection and internal use of a child’s information, but prohibiting disclosure of that information to third parties; in cases where the disclosure is integral to the site or service, this must be made clear to parents.
- Provide parents with access to their child’s personal information to review and/or have the information deleted, and give parents the opportunity to prevent further use or online collection of a child’s personal information.
- Maintain the confidentiality, security and integrity of information that is collected from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security.
- Retain personal information collected online from a child only for as long as necessary to fulfil the purpose for which it was collected, and delete the information using reasonable measures to protect against its unauthorized access or use.

For the full requirements on complying with COPPA, see <www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>.

### 6.1.3 Personal data collection

**Assessment criteria/indicator:** The company ensures that data collection, storage and sharing meet legal requirements, including parental consent requirements, and is transparent on how personal information will be used.

**Risk scenario:** Children inadvertently provide personally identifiable information and other data, which could put them at risk or be used to defraud them and/or the bill payer. Undetected sharing of personal information by children under age 13 can lead to sanctions, fines, loss of Safe Harbor certification and loss of consumer trust.

**Guidance/recommendations:** Many elements of the guidance above relating to compliance to the US COPPA Act are valid for all users regardless of user age.

### 6.1.4 Geolocation data

**Assessment criteria/indicator:** Geolocation data that enable the user’s current physical location to be identified are not collected without user or parental consent, as appropriate, and the company clearly identifies why it collects this data.
### 6.1.5 Right to review

**Assessment criteria/indicator:** The company enables users and parents or guardians to review and, if necessary, easily correct or delete personal data and information collected, stored or shared by the company if it was provided by users under age 18.

**Risk scenario:** Incorrect or false data are held online/shared.

**Guidance/recommendations:** Transparency regarding what data are collected and stored and how these data are used are the starting points. Easy-access mechanisms to edit data should be made available to all users, with options for parents and guardians to review and edit data that were supplied by children.

## 6.2 WORKING WITH BUSINESS PARTNERS

### 6.2.1 Business partner due diligence and child rights awareness

**Assessment criteria/indicator:** The company has assessed child rights impacts and risks in relation to business partners throughout the value chain.

All partners contracted to the company are clear on the company’s values and expectations with regard to promotion of child online safety and have processes in place to implement them.

**Risk scenario:** Limiting assessments to directly controlled operations may miss significant risks, including unsafe behaviour or acts in use of the company’s products and services; potential violations of corporate policies and procedures.

**Guidance/recommendations:** Relationships with business partners throughout the value chain can be leveraged to help identify and manage child rights risks. Ensure that business partners operate to the same standards of integrity as the company.

Use a systematic approach to assessing third-party risks, and cooperatively develop plans that will enable timely implementation if child rights violations are reported or discovered, including remediation as appropriate. When minor non-compliance is found, a discussion between the party responsible for the partner relationship and contract and the third party should be initiated to identify and agree on the areas for remediation. If there are major or repeated violations, specific improvement plans with clear timescales should be jointly agreed and implemented. If these plans are not fulfilled, the ultimate sanction is to discontinue working with the partner.

### 6.2.2 Third-party CSAM notice and takedown

**Assessment criteria/indicator:** The company ensures that any third party contracted to work for the company has appropriate notice and takedown procedures regarding child sexual abuse material.
**Risk scenario:** Users of products and services are able to access illegal content through third parties linked to the company.

**Guidance/recommendations:** Where appropriate, consider requiring the implementation of a simple and highly visible ‘report abuse button’ that takes users through to the reporting mechanism. Put in place an effective filter to sift malicious but non-illegal and potentially illegal content reports, and ensure all reports are swiftly passed through to an enforcement agency or hotline for review. Any decision on illegality should be made by a competent legal authority and be free of political, commercial or other unwarranted influences.


### 6.3 ADVERTISING, MARKETING, AND PROMOTION

#### 6.3.1 Terms and conditions, including for local markets

**Assessment criteria/indicator:** All customer contracts include terms and conditions that explicitly forbid accessing, sharing and storing child sexual abuse material and other illegal content/behaviour.

All terms and conditions, as well as user advice, is reviewed so that it is context-specific to local markets.

**Risk scenario:** Missed opportunities to clarify unacceptable use of products and services and contractual provisions regarding illegal behaviour; failure to account for risks in specific local operating contexts.

**Guidance/recommendations:** Use terms of service and conditions to prohibit illegal content and behaviour, highlighting that:

- Illegal content, including child sexual abuse material, will not be tolerated.
- The company will cooperate fully with law enforcement investigations in the event that illegal content is reported or discovered.
- The company is committed to international human rights standards and law, and will not unnecessarily prohibit the free flow of information on the Internet.

Engagement with local markets and availability of Internet content for children in local languages will help ensure a safer environment, and expand the benefits for all customers.

Consider partnering with local experts such as children’s non-governmental organizations, charities and parenting groups to help shape the company’s messaging and reach the intended audience.

#### 6.3.2 Advertising and promotion for products and services

**Assessment criteria/indicator:** The company ensures that all advertising, marketing and promotions are clearly identified as such, and has established clear limits for online advertising to children.

All commercial content is reviewed, including in forums, social networks and gaming sites. And the company follows national or international legislation and implements appropriate standards and rules to protect children from age-inappropriate advertising.
**Risk scenario:** Children misinterpret advertising or do not realize that the content is promotional, and make ill-informed decisions as a result.

**Guidance/recommendations:** Clearly distinguish advertising/commercial content from other content and implement measures to avoid exposing children to inappropriate advertising in any form of online media. Laws covering advertising to children vary by region and country. Ensure that the local operating context is considered when developing advertising and promotional or marketing campaigns.

### 6.3.3 Pricing transparency

**Assessment criteria/indicator:** The company ensures clear information is provided on the price of any product or service including for 'in app' purchases and for cumulative purchases and that appropriate payment consents are obtained.

**Risk scenario:** Children will run up large bills or fees by accessing products, services or features without the consent of parent or caregiver.

**Guidance/recommendations:** Transparency in fees and charges is the first step to reducing this risk. Asking for consent to make payments is another option. The company avoids addressing children directly and encouraging them to buy virtual goods or credits with their mobile phone or other means that do not require prior parental control. Contextual early warnings about additional costs are provided to empower children and parents.

### 6.3.4 Default settings

**Assessment criteria/indicator:** The company avoids default settings that would easily allow children to access premium services for which additional payment is necessary.

**Risk scenario:** Children access non-stage appropriate content that requires additional payment. Payments are taken by default rather than under verified parental consent.

**Guidance/recommendations:** Provide age-appropriate content sharing and visibility settings, for example, making privacy and visibility settings for children more restrictive than the settings for adults by default. Even where services are designed for the contracting adult, a company should assume children might use or try to use the services. For other uses, care should be taken not to infringe on human and child rights such as freedom of expression and access to information and sources of education.

### 6.3.5 Public spaces

**Assessment criteria/indicator:** When the company offers Internet access in public spaces, e.g., via Wi-Fi, it assumes children will be using those services and has the appropriate safeguarding mechanisms in place.
**Risk scenario:** Child safeguards and control requirements are not uniformly addressed across all access technologies.

**Guidance/recommendations:** To avoid child-safeguarding gaps, proactively block access to web addresses known to contain content that is inappropriate for a wide audience, in addition to blocking access to child sexual abuse material.

Include clauses in terms and conditions of use that forbid using Wi-Fi services to access or display any material that is unsuitable in an environment where children are present. These terms and conditions should include clear mechanisms regarding the consequences of infringing such rules.

Take all measures to protect against unauthorized access, such as manipulation/loss of personal data. Provide procedures and software to assist in the control and monitoring of children’s access to Internet content, and install filters on the Wi-Fi system to reinforce the company’s policy on inappropriate material.

### 6.4 CONTENT

#### 6.4.1 Content classification

**Assessment criteria/indicator:** The company develops and adapts products and services to include a classification or age rating system that will guide users, parents and teachers in safeguarding children. This includes:

- Ensuring that the classification system is consistent with national and international standards for other media.
- Providing information on the type of content if content classification standards do not exist and the content is developmental stage sensitive.
- Supporting research and development of new age-verification systems.

**Risk scenario:** Children and parents do not realize they are accessing stage-inappropriate content.

**Guidance/recommendations:** Developing products and services with age classification systems in mind reduces the risks of products and services falling into a classification that they were not developed for, and helps maximize age-targeted market potential. Working with others in the industry and with international initiatives offers an opportunity to develop a suitable system that the company can apply.

Provide an easy-to-understand guide to appropriate content for children, other users, and parents and caregivers. Include advice and reminders about age-classification of content for the online environment as well as more traditional forms of media.

#### 6.4.2 Information for parents

**Assessment criteria/indicator:** The company provides information about a service to highlight the benefits the child would obtain by behaving well and responsibly, such as using the service for creative purposes.

**Risk scenario:** Missing an opportunity to build trust and brand preference with users.

**Guidance/recommendations:** Online products and services offer great new opportunities to learn and to enhance childhood experiences. For example, online platforms can promote children’s right to express themselves, to facilitate participation in public life and to encourage collaboration and entrepreneurship. These features should be highlighted in information to parents to enable them to better understand some of the benefits use of ICT’s can bring.
6.4.3 Age-appropriate guidance and clear terminology

**Assessment criteria/indicator:** All advice provided to children is clear and understandable for the relevant ages/developmental stages.

For users, parents and teachers, the company provides a glossary or defines technical terminology at point of use, in clear easy-to-understand language. For children and young people, the language used to define technical terms is stage appropriate.

**Risk scenario:** Customers do not understand how to use ICT products or services, and are not aware of the potential risks associated with the use of technology.

**Guidance/recommendations:** Tailor instructions for different ages and developmental stages. Educate customers on responsible use of products and services and how to protect their personal data. COPPA, for example, defines personal information as:

- first and last name, telephone number, social security number or equivalent, numbers from local identity cards;
- home address, names of street or city; geolocation information sufficient to identify street/city names;
- names of pets, friends, family members, schools;
- photograph, video or audio file that contains a child’s image or voice;
- online contact information, screen or user name that functions as online contact information; a persistent identifier that can be used to recognize a user over time and across different websites or online service;
- information concerning the child or the parents of that child that the service provider collects online from the child and combines with an identifier noted above.