ICT COALITION

First Report on the Implementation of the ICT Principles

2014
April

Brian O'Neill
Dublin Institute of Technology

designed by: www.create.ie

Copyright © Dublin Institute of Technology, 2014

Centre for Social and Educational Research
Dublin Institute of Technology
41 Mountjoy Square
Dublin 1

Tel: +353 (0)1 402 4176
E-mail: cser@dit.ie
Web: www.cser.ie

Published by Dublin Institute of Technology

ISBN 978-1-900454-55-1

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission in writing of the copyright holder.

For rights of translation or reproduction, applications should be made to The Director, Centre for Social and Educational Research, Dublin Institute of Technology, Dublin 1, Ireland.

The ICT Coalition for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU

First Report on the Implementation of the ICT Principles

Brian O'Neill
Researcher: Thuy Dinh

Dublin Institute of Technology
2014

Foreword

It was a core commitment from the outset in 2010, when discussions began on the formation of an ICT Coalition spanning the whole ecosystem of internet-connected devices and online services, that any such self-regulatory initiative would need to demonstrate its commitment to independent assessment of its members' achievements in online safety, given the concerns of the public and other stakeholders in this area. This report is the first such assessment, carried out by Dr Brian O'Neill, two years after the formal launch of the ICT Coalition - a timely moment to review the achievements of ICT Coalition members, assess the state of play in the area of online safety policy and consider what the key areas for further consideration and action should be in the next few years.

Given the diversity of its membership, there are inevitably differences in the way in which companies have implemented the core Principles of the ICT Coalition, and this report should be read in conjunction with the reports of individual member companies http://www.ictcoalition.eu/commitments) to obtain a fuller picture of the detail of company initiatives. Nevertheless, it is clear that ICT Coalition members recognise their own responsibilities and will continue to be vigilant in making their products and services as safe as they reasonably can be, while allowing industry to innovate and provide opportunities for society to benefit in both social and economic terms from all that the internet has to offer to young people. We look forward to continuing constructive dialogue on these issues in our regular Stakeholder Forums in Brussels, and to working within the partnerships which form the foundation of the ICT Coalition to enhance the opportunities available to young people from a rapidly-evolving online world.

Table of Contents

List of Figures

List of Tables

List of Summary Tables

Executive Summary

The ICT Coalition for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU (the ICT Coalition) has resulted in important achievements of commitment and implementation of fundamental principles of child online safety.

1. Good progress has been made in ensuring that online content that may be unsuitable for children or young people – where available on members' services – is clearly flagged and accompanied by appropriate labelling guidelines.

2. Parental control solutions are now well established as a core element of most member companies' provision, with well-resourced information and guidance about their use and the role parents can play in managing access, particularly by younger children.

3. Reporting tools, similarly, have become essential elements wherever content is uploaded, posted or shared. Companies have also established robust internal procedures to handle reports of misuse, abuse or violations of terms of service.

4. Companies have demonstrated a solid industry consensus on tackling child sexual abuse images online. Well-established, rigorous procedures are in place, and there is clear evidence of effective cooperation with hotlines and law enforcement.

5. ICT Coalition members have given serious attention to implementing industry-standard approaches to privacy protection. Content-sharing and social media platforms have incorporated a wide range of flexible and customisable privacy settings that can be adapted to suit individual user needs.

6. ICT Coalition members have contributed extensively to educational and awareness-raising support. Across each of the themes of the ICT Principles, it is clear that companies have supported individual initiatives with information and resource material across their platforms. There are also some strong examples of collaboration with external partners, which demonstrate the potential to work collectively on raising awareness and developing skills in the area of safety.

7. Mobile use of the internet with fast-evolving applications and devices, and expanding adoption by children and young people, poses new areas of challenge. It is less easy, for instance, for parents to monitor and supervise young people's internet access in the way that they might with desktop computers in a home environment. Parental controls for the mobile environment, therefore, require further development and testing. Some companies have begun to introduce their own or third-party solutions. Progress to date, is uneven, however.

8. Members of the ICT Coalition use recognised content labelling or classification systems to label content such as own and third party, professionally-produced content for linear and non-linear services. However, this is not fully implemented in all cases. The type of classification applied varies according to the nature of the content involved and the platform on which the content is offered. Individual companies have committed, in line with national requirements, to further development of labelling guidelines in relation to apps and other commercial content. Approaches to classification of user-generated content remain an area of work in progress for the industry.

9. Online safety approaches that apply to the PC 'desktop' world translate unevenly to the mobile environment and especially to the area of privacy protection. The GSMA Mobile Privacy initiative is an important step in promoting an industry-wide approach to privacy for mobile devices and apps design. Interdependence between the diverse actors involved makes implementation more challenging.

10. The ICT Principles have been formulated in a general way so as to be flexible and capable of adaptation as the environment evolves. However, this generality means that they can be interpreted in quite different ways. It would be helpful, therefore, if in addition to supporting the Principles themselves, each company, according to the needs of its own services, developed an agreed implementation plan based on specific and measurable action. Such an implementation plan could be rolled forward on a periodic basis.

11. A singular achievement of the ICT Coalition has been the creation of a forum for knowledge exchange and sharing of experience between industry partners on internet safety developments. Sustaining this activity across the whole eco-system for connected devices should be a priority for the Coalition. Membership should be expanded where possible and emerging platforms and areas of development – including gaming platforms, device manufacturers, apps and content developers – should be incorporated. The opportunities for promoting the message of online safety on an individual company and collective level are substantial and will have wider benefits in instilling trust and confidence in the sector.

12. Further strengthening of child online safety implementation may be achieved through knowledge exchange and sharing of best practice. Sharing of information regarding the nature of reports received by companies, the take-up of parental controls and other safety features, would be an important step forward. Without compromising data protection or information regarding internal company processes and procedures, the ICT Coalition should foster further partnerships with researchers and other stakeholders to advance knowledge of new and emerging risks in the online environment.

Introduction

The internet is a vast global network that allows people around the world to connect effortlessly, to create and share their own content and to access all kinds of information on a massive scale. It offers unprecedented opportunities to transform learning, to facilitate communication and to support new forms of innovation and growth in the digital economy. The internet was designed as a free and open space without centralised control where users can enjoy a fundamental right of freedom of expression. Respecting and protecting such rights is an important responsibility of all stakeholders involved in the internet ecosystem.

There is also an important shared responsibility to protect young people and vulnerable citizens from harm when they use the internet. Through misuse or abuse, the internet can pose risks or dangers for any citizen. However, children and young people may be especially vulnerable if they do not have the capacity or the experience to protect themselves. They can be victims of bullying and harassment online; they may encounter material not suitable for their age or which may be harmful for their development; they may also fall victim to predatory contact from strangers. For this reason, ensuring children's safety online is a priority for society as a whole and something in which all stakeholders – parents, young people, educators, governments, civil society and industry – have a role to play.

A European context

Child online safety has been at the forefront of debates about the internet for nearly two decades. Europe's pioneering, multi-stakeholder approach towards creating a safer online environment for children and young people is highly regarded. From its origins with the Green Paper on the Protection of Minors and Human Dignity (European Commission, 1996) and the development of the first Safer Internet Action Plan (European Commission, 1999), sustained attention has been given to internet safety as a policy theme. Key pillars of the Safer Internet Programme include combatting illegal online content, developing systems to guide internet users about potentially harmful internet content, and supporting education and awareness-raising of safety as an issue among internet users.

Industry has played a leading role in support for internet safety since the inception of the Safer Internet Programme in 1999. It has been a partner in efforts to combat illegal and harmful content and behaviour online; it has developed innovative technologies to support safer use, and it has fostered cooperation among industry players through codes of practice governing safer mobile use and safer social networking, as well as through support for education and awareness-raising efforts. More recently, industry has engaged in a proactive way through participation in a number of collaborative fora to support innovation and new developments in internet safety implementation.

The evolving internet

Over the last two decades, the internet has become one of the most important sources of information, education and entertainment for adults and children alike. As it continues to develop, use of the internet will continue to grow and provide yet more innovative services, with social benefits as well as potential risks. While it is difficult to predict exactly how the internet will evolve, or to anticipate all the consequences that will arise from users' interaction with technology, protecting young people in the communications and media environment has been and is likely to remain an important policy objective.

In the near future, as the European Commission's Green Paper on convergence attests (European Commission, 2013), the distinction between devices such as PCs, TVs, tablet devices and laptops will erode, as consumers access and enjoy the same content across different platforms. The functionality to be found in diverse connected devices will effectively merge. Access to content and networked communications will be pervasive as technology strives to create an ever-richer, seamless experience, as users effortlessly switch between devices, providers and applications.

The evolving internet will not only be about consuming rich content on-demand. Platforms will continue to evolve that enable users to create and effortlessly share their own content and allow them to communicate widely with circles of friends and contacts. A myriad communication tools and devices will allow users to be connected and to access and communicate with contacts anywhere and at any time.

Widening use of multiple connected devices, both at home and while out and about, therefore, provides the context in which manufacturers, network operators and connectivity providers as well as online content and service providers seek to ensure ongoing commitment to child online safety.

Risks and online safety

The need for high standards of online safety will be of increased importance in this new converged environment as new services and technologies compete for consumer attention. Alongside the many opportunities created, there may also be additional risks that will require ongoing attention by stakeholders – policy makers, industry, educators, and young people themselves – to ensure young people's safety online. Patterns of risk may also evolve as new ways of connecting with people and things emerge.

Content risks have been the focus of much research and policy attention for internet safety (S. Livingstone & Haddon, 2009). Content in the traditional media environment has been the subject of a graduated system of regulation, with varying levels of regulation and control according to the context in which young people are likely to consume content. The evolving nature of the internet, however, creates a more complex environment for accessing content, raising concerns about potential access by children and young people to material that may be inappropriate or harmful for their development.

As children engage more interactively in their online use, the likelihood of *contact risks* also increases. In the course of their online social interaction, children communicate with others they may not know offline, sometimes facing unwanted contact, harassment, or worse. While predatory contact is a rare occurrence, the risk of meeting strangers and being groomed is of major concern to parents. However, being bullied by others online remains the most common contact risk (Smith & Steffgen, 2013).

Conduct risks arise where children or young people behave in ways that may lead to potentially problematic outcomes. Computer misuse or abusing other people's information, bullying or harassing others, creating and uploading indecent or offensive images, or providing advice, for instance, on suicide or pro-anorexia sites, are ways in which problems arise in which children themselves are actors.

Research shows that content-related issues including potentially harmful content such as pornography and gory or violent content, continue to cause children and young people distress (Livingstone, Kirwil, Ponte, & Staksrud, 2013).

Commercial risks, including the use of embedded marketing and wider proliferation of commercial content and advertising, are gaining in prominence as risks affecting children, particularly among younger age groups (Miyazaki, Stanaland, & Lwin, 2009). Micro payments and in-app purchases as well as potential risks from gambling and illegal downloading are areas requiring increasing attention.

The *management of personal data* in relation to children's online communication is similarly an area that will grow in importance (Shin, Huh, & Faber, 2012). Greater transparency regarding the collection, processing and transfer of personal data is an area of ongoing concern for policymakers. Young people need to be empowered to make informed choices about the sharing of personal information, particularly when using smartphones and tablets, and to be able to responsibly manage their data and online presence.

The ICT Coalition

The ICT Coalition for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU is a self-regulatory consortium of internet companies. It represents the full value chain of content, services and devices. It brings together for the first time key industry players from across the communications and internet market including connectivity platforms, online services and connected gaming and mobile devices. Currently there are 22 members. The members pledge to encourage the safe and responsible use of online services and internet devices among children and young people and to empower parents and carers to engage with and help protect their children in the digital world.

In January 2012, the ICT Coalition announced a set of guiding principles for the development of products and services to actively enhance the safety of children and young people online.

With a focus on the areas of: *content; parental controls; responding to abuse/misuse; child abuse material or illegal contact; privacy and control; and education and awareness,* signatories to the principles have committed to:

- Developing innovative ways of enhancing online safety and encouraging responsible use of the internet and internet access devices by children and young people
- Empowering parents and carers to engage with and help protect their children
- Providing easily accessible, clear and transparent information about online safety and behaviour
- Raising awareness of how – and to whom – to report abuse and concerns

Uniquely, the ICT Coalition includes member companies from across the full spectrum of online service provision, content provision, network operation and manufacturing. Accordingly, the ICT Principles have been set at a conceptual level to enable the widest participation and to ensure that child online safety is incorporated in all dimensions of the technological environment. The ICT Principles also aim to provide a long term roadmap for safer innovation, development, and product and service implementation. The Principles are complementary to existing self-regulatory initiatives (such as the European Framework for Safer Mobile Use by Younger Teenagers and Children, the EU Safer Social Networking Principles and the GSMA Mobile Alliance against Child Sexual Abuse Content).

Similarly, members of the ICT Coalition have participated in the work undertaken by the CEO Coalition for a Better Internet for Kids established by European Commission Vice-President Neelie Kroes in 2012. Sharing common goals and interests in achieving progress on implementation of standards in online safety, ICT Coalition members have supported these and related initiatives while continuing to develop the long-term roadmap for online safety.

Assessment of the ICT Principles

An important action of the ICT Coalition was the commissioning of an independent review of the implementation of the Principles. This provides the context for the current report. In 2013, Dr Brian O'Neill, Dublin Institute of Technology was appointed as independent assessor for the ICT Coalition. Terms of reference for the project included the requirement to carry out an independent assessment of the company self-declaration reports submitted by each Coalition member on their company's implementation of the ICT Principles. While the ICT Principles set out the broad objectives outlining members' obligations to online safety provision, the process incorporates specific commitments made by companies in their statements, reflecting specific benchmarks and individual targets that each company has identified under the respective headings of the ICT Principles.

The assessment report involves a thorough review of how each company has implemented specific measures under the ICT Coalition process. In reviewing companies' self-declarations, comments and observations were invited from third-party stakeholders and children's NGOs. Companies were encouraged to engage in an ongoing dialogue to discuss their plans with their key stakeholders throughout the implementation period. As a result, the ICT Coalition hosted a series of public meetings with stakeholders to discuss current issues in online safety. The final report takes account of the above-mentioned declarations and observations, and makes an overall assessment of companies' implementation, while highlighting related technological or user trends that affect this fast-moving environment.

ICT Coalition members' self-assessment reports provide an overview of implementation status

Signatories of the ICT Principles have made a significant effort, as measured by the individually announced targets in companies' implementation plans. However, keeping in mind the often ambitious targets, not every target could be reached by every member within the first year. Nevertheless, ICT coalition members are stilll committed their individually announced targets under the ICT Principles and will follow them up. For a detailed view on the implementation status of specific measures, please see the individual review reports published by each company on the ICT Coalition website.

Content

At a glance +

Signatories should:

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

Principle 1 of the ICT Principles deals with the safety issues for children that arise through the pervasive access to online content. Under this principle, signatories commit to indicate clearly where a service may include content that could be considered inappropriate for children and to provide mechanisms to restrict access to the service where such content is available. For services that include hosting or sharing of user-generated content, ICT Coalition members commit to present clear guidelines as to what is acceptable and to offer options to report content that breaches a company's content policy or terms of service.

The primary objective of Principle 1 is to give parents greater control over access to online content that may be age-inappropriate. It includes a commitment to empower users to take action where they come across material that contravenes the terms of service of a hosting provider. It also stipulates that users should have clear guidance as to what is permissible when posting or sharing content online.

Principle 1 is framed in a general way so that it may be flexibly adapted to the distinct services represented by companies in the ICT Coalition. Its implementation will therefore vary according to the content or service involved.

For the purposes of this assessment, companies were asked to supply evidence of how they had implemented Principle 1 and to include details, where applicable, of mechanisms to restrict or block access to age-inappropriate content. The companies were also asked to identify relevant reporting options available to report breaches of content policy.

Content, as Table 1.1 illustrates, is relevant in some form or other to all of the companies in the ICT Coalition. Content is now a ubiquitous element of internet experience and, regardless of where in the value chain a company's area of activity may be located, content-related issues increasingly arise in a company's implementation of internet safety.

Figure 1.1

ICT Coalition companies

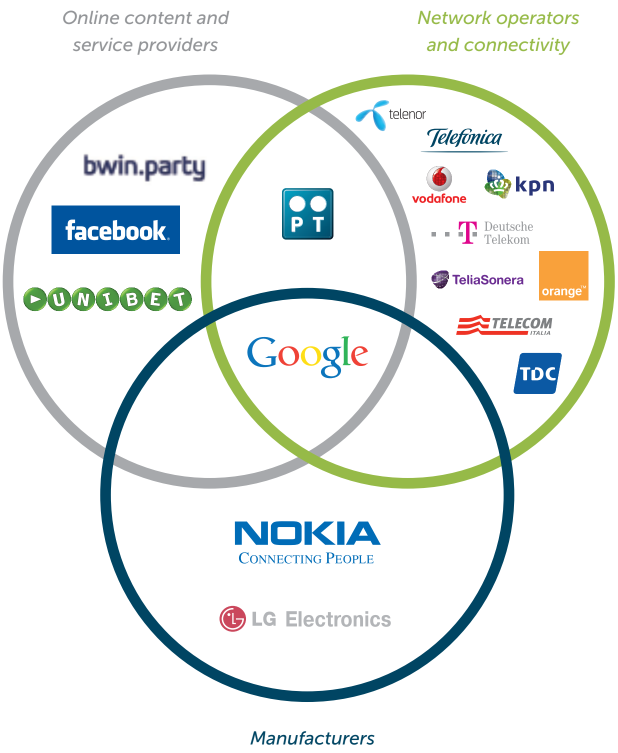


Table 1.1

Types of content

Type	Company
IPTV services/Video on-demand	Deutsche Telekom, KPN, Orange, Portugal Telecom, TDC, Telecom Italia, Telefónica, TeliaSonera, Vodafone
Own or third party apps, other commercial content	All (except TDC)
User-generated content	Facebook Google Portugal Telecom
Communication/Chat Content	Orange, Unibet, Google, Facebook, Telecom Italia, Portugal Telecom
Cloud-hosting services	Deutsche Telekom, Vodafone, Portugal Telecom, Telecom Italia

Across the 16 companies included in this assessment (Figure 1.1), each has a relationship to content either directly as a content provider, network operator or connectivity provider (with more limited content provision), or as a manufacturer of devices to access content.

Content, for the purposes of this assessment, is divided into three main categories: IPTV/video on-demand services; own or third party apps, or other commercial content; and user-generated content including cloud storage facilities.

Ten of the companies in the assessment group are primarily network or connectivity providers. Many of these also provide content in the form of apps or other mobile content on their own platform or via the Apple App Store or Google Play store. Additionally, eight of these companies also offer IPTV services, a different form of content that also falls under the regulatory regime for broadcasting or video-on-demand services. Three companies – *Google, Facebook and Portugal Telecom* – offer platforms for user-generated content. Chat functions and communications content represent a different type of content. Finally, cloud hosting facilities for sharing user-uploaded content are offered by *Deutsche Telekom, Portugal Telecom* and *Vodafone*.

Access to content

Companies commit as part of Principle 1 to indicate where their service may include content that may not be suitable for children and young people, and to display prominently available options to control access.

All companies were found to comply with the requirement to indicate where a service may contain content that is unsuitable or age-inappropriate for children (see Summary Principle 1, p.19). In practice, a diversity of methods is used to indicate if content may be unsuitable, depending on the nature of the service. The following were the principal methods identified:

- In the case of IPTV services, content is age-rated and access controls as required by national legislation are typically used.
- Own or third-party content is generally labelled according to a standard classification system such as the Pan European Game Information (PEGI) or in-house classification scheme.
- In the case of Unibet and Bwin.Party, all gambling content is flagged as suitable for over-18s only and appropriately age-gated.
- User-generated content is subject to company policy. After content has been flagged, it is reviewed and action is taken in accordance with company policies. This includes the provision that content that does not violate TOS, but is deemed to be not suitable for children is moved to the over-18s category.

While a requirement for content classification is not formally included as part of the ICT Principles, companies undertake to provide clear notification through an advisory notice or a labelling scheme that can guide parents or carers when unsuitable content may be present. Wider use of content classification is evident among most of the companies and services reviewed.

Companies also undertake to display prominently controls to limit access to content that may be unsuitable for children. With regard to options provided for access control, the manner of implementation depends on the nature of content involved.

The options provided by companies were reviewed under the three distinct headings of: (a) IPTV services or video-on-demand services; (b) Own or third-party apps, other commercial content; and (c) User-generated content and cloud hosting services.

IPTV services or video-on-demand services

Eight companies offer IPTV or video-on-demand services. Such services are typically regulated according to national requirements as provided for in European audiovisual legislation.

- All providers of IPTV services include PIN-controlled access tools where content may be age-inappropriate.
- In addition, providers offer parental control tools with options to restrict age-rated content (see Principle 2 for further details).
- Where content is of an adult nature, age verification procedures are followed in accordance with national requirements.

Own or third-party apps, other commercial content

All but one of the companies included in the assessment offers commercial, professionally produced, own or third-party content either in the form of apps, gaming content and gambling content through either online, fixed or mobile platforms. In this context, Principle 1 is relevant to all companies.

- All companies were found to provide some forms of control mechanism to restrict access to content that is age-rated.
- All providers include advice to users, in the form of online educational resources or information about company policy in relation to content.
- Most companies use a recognised content labelling or classification system to label content though this is not fully implemented in all cases. The type of classification applied varies according to the nature of the content involved and the platform on which the content is offered. There are also national requirements for age rating of mobile content or premium services but the way in which this is implemented varies.

User-generated content/cloud hosting services

Five companies offer platforms for user-generated content or cloud hosting services. This is limited in the case of connectivity companies such as Deutsche Telekom and Orange, somewhat more substantial in the case of Portugal Telecom, and, of course, a core feature for Facebook and Google.

- In the case of Orange, content generated by users is limited to chat functions located within forums, and is governed by rules of appropriate conduct.
- Companies within the Deutsche Telekom Group do not offer user-generated content as such but rather cloud hosting services whereby users may upload and share their own content.
- User-generated content available through Portugal Telecom services (SAPO Videos, SAPO Fotos, etc) is age-rated with access controls available to restrict viewing by under-age users.
- The sharing of user content is at the core of the service offered by Facebook and is governed by terms and conditions for all content creators. Facebook's Statement of Rights and Responsibility outlines the relevant terms for user content. Content that is unsuitable for minors must be age gated to 18+.
- Google through its YouTube services offers a platform for sharing user-generated content. Age restrictions are primarily imposed by users rather than as a result of a review by YouTube though Google may still choose to restrict access to content. Content that is age-restricted by users is still subject to the YouTube Community Guidelines and can be flagged by members of the YouTube community. Age-restricted content requires users to be logged-in to view.

User policies

As part of their commitment to provide users with guidance and clear information about the nature of the content services offered, members of the ICT Coalition undertake to provide easy-to-understand Acceptable Use Policies (AUP) in an accessible location. Under this requirement, companies, as a minimum, provide general Terms and Conditions for users of services. The assessment confirmed that such Terms, as appropriate to the service concerned, are displayed in prominent locations, typically placed in the footer of the relevant webpages. Where services involve hosting of content or user-generated content, specific conditions applying to content and user behaviour are stipulated (these are reviewed below). Companies undertake to state clearly any relevant terms of service or community guidelines (i.e. how users are expected to behave and what is not acceptable) with which user-generated content must comply.

Not all companies in the ICT Coalition provide services or platforms that allow user-generated content and therefore not all companies specify in their terms of use the specific requirements or guidelines regarding user behaviour. Nine of the 16 companies do include a statement regarding responsibilities of users when creating or sharing content.

- LG Electronics as an equipment manufacturer; connectivity companies TDC, Telefónica, Telenor, TeliaSonera and Vodafone; and service providers Unibet and Bwin.Party do not provide platforms for user-generated content; thus this requirement is not applicable.
- In cases where there is limited scope for user interaction or user-generated content, user terms are confined principally to rules of netiquette in online forums; for example, Orange and Telecom Italia.
- Companies such as Deutsche Telekom, Vodafone and KPN which include hosting services require users to agree with terms of use for content and behaviour that is permitted on the relevant services.

Portugal Telecom, Google and Facebook provide platforms where users can create and share their own video, audio and photographic content. In these three instances, detailed user policies were supplied along with relevant supporting material guiding users as to what is acceptable and permitted on the platform.

- Portugal Telecom's platforms (SAPO Videos, SAPO Fotos, MEO Kanal) are supported by a centralised safety page that also links to the relevant areas of the service. Clear guidelines are provided as to what is permitted, including details related to the nature and ownership of content, as well as consent in the case of minors.
- Google describes the community guidelines on YouTube as its "rules of the road". They outline what is unacceptable and what is prohibited (bullying, hate speech, spam) on the platform. User guidelines were found to be written in easily accessible language. They are supplemented by the YouTube Policy and Safety Hub which provides additional resources about the conditions and requirements on the platform.

- Facebook provides a Statement of Rights and Responsibilities for Users in its policy resource pages written in accessible and easy-to-understand terms.

Consequences of violations of terms

In the same way that companies undertake to provide information and easily accessible terms of service for users, so too they commit to provide notice of the consequences for users if they post content that violates terms of service or community guidelines.

This requirement is of primary relevance to companies that provide platforms for user-generated content:

- In the case of Google, guidelines and content policies outline penalties that apply up to the termination of an account, which in the case of YouTube encompasses a three-strikes policy within a six-month period following which a user's account will be terminated.
- Facebook's Statements of Rights and Responsibilities includes reference to actions that may be taken by the company in response to breaches of its terms including the right to remove content, disabling all or part of a user's account or deleting it.
- Portugal Telecom details conditions under which access will be suspended or an account cancelled on its SAPO Video or SAPO Foto platform. Similarly, on its Meo Kanal, Portugal Telecom reserves the right to remove any content that may be "offensive to good manners, illegal, malicious, pornographic, violent, discriminatory, offensive, or that violate the privacy of other parties".

Reporting options

The provision of reporting tools in relation to abuses of services is considered under Principle 3. Reporting, in this context, refers to the options available in the relevant areas of a company's service for users to notify or file a complaint about content, its age-appropriateness or the manner in which it has been classified. Signatories undertake to provide opportunities for users to provide feedback on content, whether that is own or third-party material or user-generated content.

Own or third-party content

First, in relation to the provision of content that is commercial or professionally produced (and noting that content is relevant to all companies in some form or other), all but two of the companies confirm that they provide options for reporting or filing a complaint in relation to own or third-party content.

The principal way in which reporting is facilitated is via a report button or flag placed adjacent to the content or within the app store. Clicking on a report button typically provides a link to a report form with pre-formed categories to classify the nature of the complaint. Some reporting tools include a text field for additional comments and the email address of the complainant.

Many of the companies also provide an alternative means of reporting or providing feedback such as providing links to their customer service teams. In two cases, insufficient information was provided or no apparent reporting option was identified.

Table 1.2 gives a breakdown of the reporting options provided.

Table 1.2

Reporting options, own or third-party apps

Reporting Option	Company
Report button in app store or placed alongside content	Facebook, Google, Nokia, Portugal Telecom
Link to customer services or other feedback channel	Deutsche Telekom, KPN, Orange, Portugal Telecom, TDC, Telecom Italia, Telefónica, Telenor, TeliaSonera, Unibet, Vodafone
No reporting option indicated	Bwin.Party, LG Electronics

In the case of Bwin.Party, while it is noted that minors are excluded from content which is rated in its entirety as suitable only for over-18s, no information was provided about a mechanism to report content nor was it possible to identify one on Bwin.Party's service.

LG Electronics does not make its own content, but through LG Smartworld it offers a range of apps and content for smartphones and smart TVs. Content is rated according to standard classification guidelines. However, no information was provided about a mechanism to report content nor was it possible to identify one on the service.

User-generated content

The second category of content for which signatories commit to provide a reporting mechanism is that of user-created and shared content over which the company typically does not have control, but where it provides tools or mechanisms by which users can flag or report material that may be inappropriate.

This is applicable to seven of the companies in the ICT Coalition:

Table 1.3

Reporting options, user-generated content

Reporting Option	Company
Report option available for user-generated content and cloud hosting services	Deutsche Telekom, Facebook, Google, Nokia, Orange, Portugal Telecom, Telecom Italia
Not applicable No platforms for user-generated content	Bwin.Party, LG Electronics, KPN, TDC, Telefónica, Telenor, Telia Sonera, Unibet, Vodafone

Reporting options, dealt with also under Principle 3, typically comprise a tool to flag or report content, using a combination of predefined categories with additional information supplied by the user. Features of the reporting mechanisms provided by companies in this sample include the following elements:

- Deutsche Telekom's consumer cloud and hosting services include an online reporting tool that allows users to report inappropriate content. The company stipulates that for all such services, the reporting tool should be easy to find and use. Anonymous reports are not allowed and an email address is required on submission of a report.
- Facebook, incorporates a tool to report any content that breaches its terms of service. All reports are reviewed. It also provides a 'social reporting' tool. This enables a user to report directly to the person who posted the content in instances where the material does not violate Facebook terms but that offend or bother the complainant.
- Google's principal reporting mechanism in this context is the community flagging system on the YouTube platform. Flagged videos are reviewed for compliance with YouTube's Community Guidelines and, if found to be in violation, will be removed. If not a breach of YouTube terms, content may also be age-restricted.
- Portugal Telecom's reporting buttons are available within the relevant services for video and photo sharing, and enable users to report against pre-defined categories including mislabelling of content. Users may also include comments in a text box.
- Nokia is in the process of implementing a content classification scheme for the Nokia Store. A report button is included that allows users to report any content against categories of: Obscenity, Violence, Abuse, Spam, Fraud, Racism or Other. Report tools and handling procedures are similarly available for any applications including the Here/Maps services where it is possible to provide user generated content.

Providing innovative solutions

Given the rapidly evolving context in which internet content is made available and shared across diverse networks, devices and platforms, companies also undertake as part of Principle 1 to continue to work to provide innovative solutions to support internet safety for children and young people.

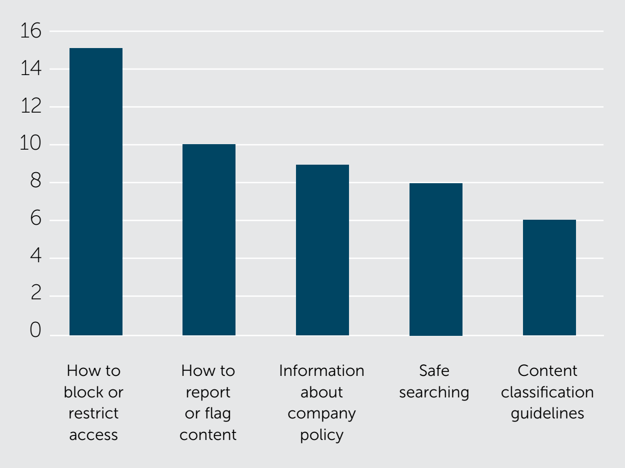
In the first instance, companies were asked to indicate where they had provided any information, educational resources or advice for users, with specific reference to content. Figure 1.2 presents an overview of the kinds of resources and educational content provided.

In line with one of the main requirements of Principle 1, 15 of the 16 companies (no information was supplied by Telefónica) give information about how to block or restrict access to content. Secondly, most companies do provide information about how to report or flag content as inappropriate. Fewer (six out of the total) provide information about content classification or labelling guidelines.

Innovation is evident in examples cited by ICT Coalition members of new implementation of access controls, especially on mobile devices, content classification and in reporting mechanisms. Given the rapidly evolving context for content sharing, this remains an area where new solutions will be required.

Figure 1.2

Information resources



Summary

Principle 1, relating to content, receives a high level of support by companies in the ICT Coalition.

- All companies meet the requirement to highlight where a service may contain content that may be unsuitable or age-inappropriate for children. In practice, implementation of this requirement is achieved in different ways and in accordance with the nature of the content concerned.
- In some instances, local or national requirements determine the manner in which content is classified, rated and accessed (as, for instance, in relation to IPTV services or premium-rate mobile content).
- Companies have made advances in the wider use of standard content classification schemes for commercially produced, own or third-party content. User-generated content is typically classified according to the in-house terms or classification schemes developed by companies.
- All companies present easily accessible Terms and Conditions for users of services.
- Companies that offer user-generated content were found to offer clear guidance on the kind of content and behaviour permitted when uploading and sharing content.
- Consequences of violations of terms of service are clear and consistent.
- Most companies provide reporting tools for users to notify where content may be unsuitable or mislabelled, or where they may wish to file a complaint about a breach of a company's terms. Reporting buttons to file a complaint in relation to content are used by five companies. Other companies use a link to their customer services channel as the reporting option. In two cases, no reporting option was indicated.
- Reporting options for user-generated content, for media-sharing platforms and for cloud hosting services were appropriately placed and available for users.
- A range of additional resources and educational materials are available to provide guidance and support in relation to content. All but one of the companies provide additional information about how to use access controls for content. Most also provide information about reporting tools available on the service. Over half of the companies include dedicated information pages about their company's policy in relation to children.
- Promoting wider use of content classification remains an area for further development by the ICT Coalition.

Overview of selected features: Principle 1

Company	Content type	Indicate clearly inappropriate e content	Access controls	Recognised system of content labelling	Easily accessible AUP	Community guidelines for UGC	Reporting options	Consequences of violations
Bwin.Party	Apps/Other	🟩	🟩		🟩			
Deutsche Telekom	IPTV	🟩	🟩		🟩			
	Apps/Other	🟩	🟩	🟩	🟩			
	UGC/Cloud	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Facebook	Apps/Other	🟩	🟩	🟩	🟩		🟩	
	UGC/Cloud	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Google	Apps/Other	🟩	🟩	🟩	🟩		🟩	
	UGC/Cloud	🟩	🟩	🟩	🟩	🟩	🟩	🟩
KPN	IPTV	🟩	🟩		🟩			
	Apps/Other	🟩	🟩	🟩	🟩	🟩	🟩	
LG Electronics	Apps/Other	🟩	🟩	🟩	🟩			
Nokia	Apps/Other	🟩	🟩	🟩	🟩			
	UGC/Cloud	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Orange	IPTV	🟩	🟩		🟩			
	Apps/Other	🟩	🟩	🟩	🟩			
	UGC/Cloud	🟩	🟩		🟩	🟩	🟩	🟩
Portugal Telecom	IPTV	🟩	🟩		🟩		🟩	🟩
	Apps/Other	🟩	🟩	🟩	🟩			
	UGC/Cloud	🟩	🟩	🟩	🟩	🟩	🟩	🟩
TDC	IPTV	🟩	🟩		🟩		🟩	
Telecom Italia	Apps/Other	🟩	🟩		🟩	🟩	🟩	
Telefónica	IPTV	🟩	🟩		🟩			
	Apps/Other	🟩	🟩		🟩		🟩	
Telenor	Apps/Other	🟩	🟩	🟩	🟩		🟩	
TeliaSonera	IPTV	🟩	🟩		🟩			
	Apps/Other	🟩	🟩	🟩	🟩		🟩	
Unibet	Apps/Other	🟩	🟩		🟩	🟩	🟩	
Vodafone	IPTV	🟩	🟩		🟩			
	Apps/Other	🟩	🟩	🟩	🟩		🟩	
	UGC/Cloud	🟩	🟩		🟩	🟩	🟩	🟩

Note: categories refer to implementation at the group level and may not be available in all markets. See individual company reports for details.

IPTV
Apps/Other commercial content
UGC/Cloud Storage

Parental Controls

At a glance +

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

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

Parental control tools or filters have long been advocated as a way of assisting parents/guardians to manage or to restrict their children's internet access to content that may not be suitable. Some filters also allow parents to manage the amount of time children spend online or to control the kinds of applications or communications functions used. Parental controls come in a variety of configurations: they may be pre-installed or integrated within a service or device; they may be applied at the network level or router level or they may need to be downloaded and installed by users on individual devices. The wide variety of technical solutions, their perceived complexity and parents' reluctance to use monitoring or filtering devices has meant that their take-up to date has been relatively limited. While it is recognised that parental controls on their own are not a complete solution for protecting children online, and they do not replace communication between parents and children about online risks, they can, as policymakers have advocated, play an important role in managing children's internet experience.

The ICT Principles contain a commitment on the part of signatories to include parental control tools and mechanisms as part of their internet safety provision. The implementation of this commitment, as in the case of Principle 1, varies according to the nature of the company and type of activity involved. Manufacturers undertake to incorporate at a design or hardware level simple-to-use controls to limit online access. For network providers, filtering options may be offered at either network or device level, while service and content providers undertake to provide the necessary tools and settings to enable parents to manage children's online access.

For the purposes of this assessment, companies were asked to confirm the availability of parental control tools and settings on their products/services. Companies were also asked to identify the kinds of features their parental control packages contained and to describe any additional education or awareness-raising initiatives about the use of parental control tools. Companies with a wide product range or that operate in a variety of markets were asked to clarify if a common approach was adopted at corporate level or whether a different provision applied to distinct markets or product offerings. Data from each of the companies was cross-referenced and checked against the information available on the services' websites. Parental control functions as identified by the companies were inspected and verified according to the information submitted.

The following summary outlines the range of parental control tools offered by members of the ICT Coalition and assesses it against the commitments given under Principle 2 to *make available the necessary tools and settings which simply and clearly help parents to set appropriate levels of control.*

Availability of parental controls

All but three companies comply directly with Principle 2 through provision of parental controls. Each of these companies has adopted a corporate, group-level policy approach to the provision of parental controls.

Principle 2 is of limited relevance to the services of Bwin.Party and Unibet. Both promote third-party parental control tools on their websites for parents who want to make sure that gambling content is inaccessible on their computers. In addition, age verification methods as required by national gambling legislation may also be considered to serve as parental controls.

In the case of Facebook, parental controls are not directly offered within the platform. However, pages containing material suitable only for over-18s must be age-gated. Facebook also promotes parental engagement in young people's online social media presence through a variety of help resources dedicated to the topic.

For those companies that do offer parental control solutions, the particular approach may vary, particularly for subsidiary companies that operate in different markets. The different features made available by manufacturers, network providers (both fixed-line and mobile) and service and content providers are below considered in turn.

Manufacturers

Three companies in the ICT Coalition – LG Electronics, Google and Nokia – are manufacturers or manufacturing is part of their activities. Each includes parental controls at the level of design or hardware:

- For their smart TVs, LG Electronics integrates the option of a parental PIN code restricting access to channels and to content. For their range of smartphones, an Android-based parental control tool, available for download from the Google Play store, is provided for LG Smartphones.
- Nokia supplies a range of parental control options for its devices. These include a 'Kid's Corner' tool to set a password-protected area on a Nokia Lumia device. Browser and Store access may be blocked on Nokia mobile phones, while on Asha touch devices it is also possible to block browser access and restrict installation of apps.
- For the purposes of this assessment, Google's product range may be taken to include a range of portable devices, including smartphones and tablets. Google's Android 4.3 operating system for mobile devices includes a parental controls feature. This allows the tablet/phone owner to create a 'restricted profile' that limits access to features, specified content or particular applications. This feature may also be used to disable in-app purchases or push-notifications. However, the 'restricted profiles' API or Applications Programming Interface must be implemented by app developers to be fully effective and to achieve this full level of control.

Network providers

Ten of the companies in the ICT Coalition are network operators or connectivity providers which offer a range of fixed-line and mobile communications services. In fulfilling their commitment to offer parental controls across the range of services, different options are provided according to the nature of the service and the markets being served.

Fixed-line internet access is offered by all 10 network/connectivity companies. All assessed providers have a parental control solution in place as part of their offering. In addition, a range of options are provided, including:

- Customisable parental control software available for download allowing the blocking of websites and managing of the amount of time spent online.
- Proprietary parental control tools such as branded products from F-Secure, Bit Defender, Norton etc.
- Some companies (KPN, Telenor) provide downloadable browser products such as *Magic Desktop*, or *MyBee* or the *juki.de* online environment developed in conjunction with Google Germany, to provide safe, 'walled garden' areas for children to use online.

In addition, those providers that offer IPTV services (see Principle 1) incorporate customisable PIN-controlled access to block adult channels, to restrict video-on-demand (VoD) purchases and subscriptions to pay-TV directly from the TV set as well as to restrict access to VoD offerings depending on the age of the child.

The mobile environment offers more challenges when it comes to deployment of parental controls. Of the 10 companies offering mobile connectivity services:

- All providers offer a basic level of control or 'child-safe' mobile package whereby parents may choose to block internet access on a child's account, to block premium-rate services and to limit calls or purchases via the mobile device.
- Within Portugal Telecom, MEO offers its MEO Kids mobile plan, the recommended plan for children with a set of safety-oriented rules and cost-controlling features such as authorised contacts, restriction on premium services, top-ups functions. TDC similarly offers a self-service, prepaid subscription aimed at children using mobile phones.
- A number of companies offer own or third-party full-featured parental control tools for download. These are typically device-based packages which enable parents to configure user profiles and manage children's internet use on a smartphone or mobile device.
- Six of the companies (Deutsche Telekom, Orange, TeliaSonera, Telenor, Telecom Italia and Vodafone) offer a full-featured parental control suite in all of the markets served by their subsidiaries. The Vodafone Guardian App is an example of good practice in this regard, with a well-configured solution which helps to manage a child's smartphone usage by protecting them from inappropriate calls and filtering SMSs, MMSs, audio, video and inappropriate apps and access to the Internet.
- Further roll-outs are planned by the Orange Group which currently offers a device-based mobile parental control package in Romania, Spain, Slovakia and Luxembourg, as well as a network-based parental control system in France.
- Parental controls for mobile devices (smartphones and tablets) are also planned by KPN and Telefónica.

Service providers

Online service or content providers occupy a somewhat different position in relation to parental controls. Of the five companies considered under this heading, two offer some form of integrated parental control mechanism, but its relevance is less for three other companies:

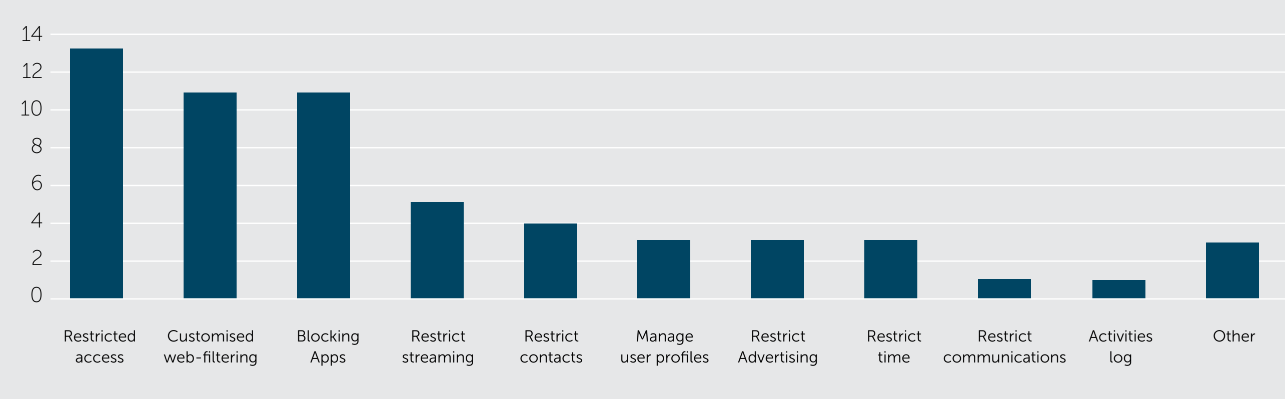
- Google offers a variety of parental control features across its services. 'Safe Search' enables the filtering of sexually explicit content from search results. YouTube 'Safety Mode' provides a similar feature for blocking age-inappropriate video content. Google has also introduced a 'Chrome Supervised User' account feature whereby users can browse the web with guidance. Safe search is also on by default for any supervised user.
- Portugal Telecom offers Bit Defender parental control software as part of its service package. Its SAPO search engine also has options available to select 'safe', 'moderated' and 'restricted' search modes.
- Facebook does not offer integrated parental control features. However, content that is unsuitable for minors must be age-gated to over-18s. In addition, Facebook also provides dedicated resources and advice directed to parents in the Safety Centre to help them talk to their child about how to manage their presence online and on Facebook.
- In the case of Unibet and Bwin.Party, as content on both platforms is only suitable for over-18s, the integration of a parental control feature is not appropriate. Both companies recommend the use of third-party parental control packages as an additional precaution for parents to ensure their children's access is blocked.

Features offered

Given the diversity of parental control solutions across the member companies, different levels of functionality in control software are apparent. Figure 2.1 provides an overview of the parental control features offered:

Figure 2.1

Parental control features offered



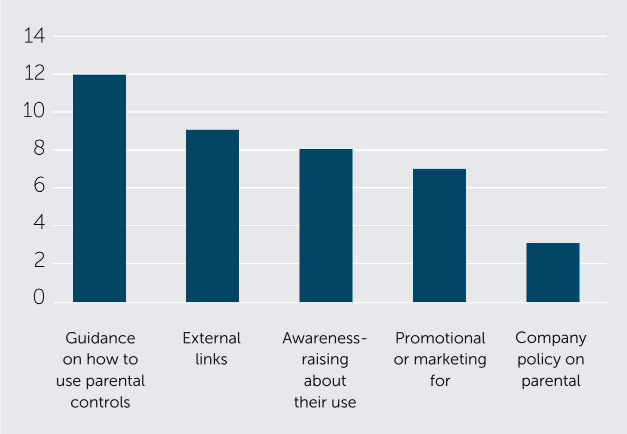
- Customised web filtering, restricting access and blocking apps are the main functions offered in the parental control toolsets. Such features are offered by 13 of the 16 member companies.
- Managing user profiles and restricting communications or contacts are features associated with dedicated proprietary parental control solutions offered by a smaller number of companies.
- Other additional features offered by specific providers include safe search modes (Google and Portugal Telecom), restricting time online (TDC, Orange) and timestamp of last log in (Bwin.Party).

Additional resources and awareness-raising

As part of the Principle 2 commitment to assist parents in managing their children's online access, companies also undertake to support the adoption of parental controls through awareness-raising, and the provision of guidance and advice about the role such tools can play in keeping children and young people safe online. The range of additional information and educational material provided by companies was also assessed and is illustrated in Figure 2.2:

Figure 2.2

Information related to use of parental controls



All companies supplying parental control solutions provide some form of guidance about their use.

The principal format for informational support takes the form of a dedicated webpage or safety channel in which information or advice about the use of parental controls was provided. Similarly, most companies provide some form of awareness-raising about parental controls or have a specific marketing channel to promote parental control products. Nine of the companies also provide links to external educational material or resources about the use of parental controls.

Training initiatives are another example of industry activity to support awareness and adoption of parental controls:

- Orange has organised a series of parent training sessions in some of its larger stores in France; according to the submission, these have reached almost 4000 customers in 39 towns across France. Training booklets and videos are also available on the website covering topics such as how to set up and customise Orange parental controls.
- Training for sales representatives and call-centre advisors on uses of parental controls as an aid to increasing internet safety is another example of work being carried out to support awareness and take-up of parental control products. In France, Orange offers an e-learning programme dedicated to child-protection available to sales representatives and call-centre advisors. Customer-facing employees in France are regularly assessed on child-protection issues.

Planned developments for parental controls

As reported by companies during the assessment process, the development of new features and products for parental controls has gathered pace in the last year with new planned rollouts during the course of 2014 particularly for mobile devices. There is an increasing demand, in the example cited by Orange, for an application that:

- Allows parents to identify and agree on the restricted access to sites that they feel are inappropriate for their children
- Informs parents of what children are searching for online and facilitates discussions with their children on what is inappropriate content
- Helps parents teach children time-management habits and agree on usage limits for online activity
- Alerts parents to when children push the agreed boundaries, e.g. if their child attempts to visit an agreed restricted website.

This is evolving work which continues to receive high priority as the market for mobile products and services increases. Implementation, therefore, needs to be reviewed on an on-going basis.

Summary

Parental controls have been recognised as an important element in contributing to online safety and have received wide support from members of the ICT Coalition.

Parental controls can be implemented at various points in the internet value chain, from core network filtering, filtering at the router level for all connected devices in a household, device controls which need to be installed and configured on individual devices, and 'profile controls' which need to be configured within individual applications, browsers or services. Parental controls can offer a variety of features to regulate access and times of usage and to restrict contacts. Rather than a crude software solution to managing young people's internet access, however, their use needs to be contextualised and supported by education, awareness and dialogue.

The review of ICT Coalition members' provision for parental controls revealed good demonstration of progress and implementation in the following:

- All Coalition members either implement parental control mechanisms and/or offer dedicated support resources for parental controls as part of their offering. However, to be fully effective, parental controls need to be available – and interoperable – at all levels of the internet value chain: from the device and OS level through to the applications used.
- Network operators and connectivity providers in this assessment offer a variety of parental control products including network filtering options, device-based downloadable products and solutions for mobile smartphones and other portable devices.
- Parental control solutions for fixed internet access are well established; a wide range of customisable solutions is available. All of the providers in this category offer a range of products, including network-level filtering, router-based parental controls for all connected devices, device-based solutions and child-friendly 'walled garden' environments.
- Given the rapid proliferation of smartphone use by children and young people, the availability of parental controls for smartphone and connected devices is of particular importance. Parental control offerings for the mobile environment are not as well developed.
- Manufacturers including LG Electronics, Nokia and Google have developed parental control features in their operating systems. Some gaps remain in the implementation for all devices and platforms and there is variation in the features offered.
- All mobile operators offer a basic level of control, with a child-safe mobile package to manage children's mobile use. Six companies offer a full-featured parental control solution for mobile devices. The remaining companies are planning further implementations while also providing support for third-party solutions.
- Content or service providers approach parental controls somewhat differently. Unibet and Bwin.Party, whose content is strictly for over-18s, advise users to implement third party parental controls to prevent access by minors. Google implements parental lock features through its 'SafeSearch' and YouTube 'Safety Mode'. It has also implemented a Chrome 'restricted Profiles' feature for its Android 4.3 operating system.
- Facebook does not offer a parental control tool on its platform. However, access to over-18s content is restricted. Facebook also includes extensive safety resources for parental guidance on managing young people's social media presence. Many of Facebook's features for minors (13-17 year-olds) are designed to remind young people of who they are sharing with and what it means to post publicly.

Overview of selected features: Principle 2

	Manufacturer		Content providers		Network/connectivity providers			
Company	Integrated	Other	Integrated	Other	Device-based	Network or router level	Mobile option	Other products
Bwin.Party				🟩				
Deutsche Telekom					🟩	🟩	🟩	
Facebook								
Google	🟩		🟩					
KPN					🟩			
LG Electronics		🟩						
Nokia	🟩							
Orange					🟩	🟩	🟩	
Portugal Telecom			🟩		🟩			🟩
TDC						🟩		🟩
Telecom Italia					🟩		🟩	🟩
Telefónica						🟩		
Telenor					🟩		🟩	🟩
TeliaSonera					🟩		🟩	
Unibet				🟩				
Vodafone					🟩	🟩	🟩	

Note: categories refer to implementation at the group level and may not be available in all markets. See individual company reports for details.

Dealing with Abuse and Misuse

At a glance +

Signatories should:

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

The provision of a simple and reliable process to report content or behaviour that breaches a service's terms and conditions is recognised to be essential to maintaining a safe online environment. Increasing internet use and sharing of content online create valuable opportunities for internet users but also produce new situations in which abuse may take place. Hence, the necessity for context-sensitive reporting mechanisms that enable users to flag content that may be inappropriate, to report online contact that may be abusive or harmful, or to report a suspected violation of community rules. Improving the mechanisms that enable users to report and the manner in which such reports are handled are matters that companies have sought to develop under Principle 3.

Member companies commit under this principle to provide reporting tools supported by appropriate and adequately resourced internal procedures for reviewing and responding to reports and to promote the availability of reporting facilities as a core part of their service.

For this assessment, companies were asked to outline how they dealt with the reporting of abuse or misuse on their services and the kinds of reporting facilities provided. Each report was assessed in turn and compiled into a combined report outlining how Principle 3 has been implemented across the members of the ICT Coalition.

Scope of company policy

As with other sections of the ICT Principles, not every aspect is relevant to each member company. The responding companies were asked to identify the scope of their policy and where relevant to indicate if the approach was taken at group/corporate level or if different solutions were taken for different markets.

Table 3.1

Group policy approach

Reporting option	Company
Group/corporate level approach	Facebook, Google, Nokia, Portugal Telecom, TDC, KPN, Telecom Italia
Group level with some variation according to market	Deutsche Telekom, Orange, Telefónica, Telenor, TeliaSonera, Vodafone
Does not apply	Bwin.Party, Unibet, LG Electronics

Seven of the companies in the ICT Coalition adopt a corporate-wide or group-level approach to the provision of tools or mechanisms to report abuse. These comprise content or service providers that operate in all EU markets (e.g. Nokia, Google and Facebook) or that are focused on a single market (e.g. Portugal Telecom, Telecom Italia). A further six companies operate a group level policy approach with variation according to individual markets or where a subsidiary company specifies its own approach individually. These consist primarily of network operators or connectivity providers which operate in a variety of markets.

Principle 3 is not relevant to LG Electronics as its principal business is as a manufacturer. It has limited connection to the services of Bwin.Party or Unibet. While both provide chat functions where it is possible that one adult customer could harass another adult customer, minors are excluded from the service. In the case of chat, a reporting function is included on the platform that issues a mail to customer services.

In terms of the scope of company policy, while reporting abuse refers to any misuse of a company's service, different approaches and emphases appear in companies' statements. Key areas of emphasis within company policy on reporting of abuse include:

- Content or contact that is Illegal (treated separately under Principle 4)
- Any content or behaviour that breaches the terms of service of community guidelines
- Content that is unmoderated or beyond the company's editorial responsibility (also covered under Principle 1)
- No specific policy as no user-generated content is involved

These different emphases, as may be seen in the individual submissions from companies, have a bearing on the kinds of reporting tools and supports supplied, and accordingly are taken into account in the assessment of different elements of Principle 3.

In terms of the kinds of content that may be reported, the general approach adopted is that anything that violates a company's terms of service may be reported. Formulations vary between specifying any harmful content, specified categories, or illegal content. Examples include:

- *Policy referring to post-/un-moderated consumer hosting services* (Deutsche Telekom)
- *Any content that breaches terms* (Nokia)
- *Potentially illegal, inappropriate content or harassment, as well as spam* (Orange)
- *Inappropriate user behaviour; Illegal content (paedophilia, violence, xenophobia); Inappropriate content; Mislabelled content; Content breaching terms of use* (Portugal Telecom)
- *P2P malicious calls or messaging. Also covers Cloud storage services. All content – reporting allows free text* (Vodafone)

Implementing a clear and simple reporting process

Companies commit as part of Principle 3 *"to the provision of a clear and simple process whereby users can report content or behaviour which breaches the service's terms and conditions".*

Thirteen of the companies in the ICT Coalition have implemented a simple and clear reporting process or mechanism allowing users to report content or behaviour that breaches the service's terms and conditions. The three companies which declared that the principle is not relevant to their product or service accordingly do not provide a reporting tool.

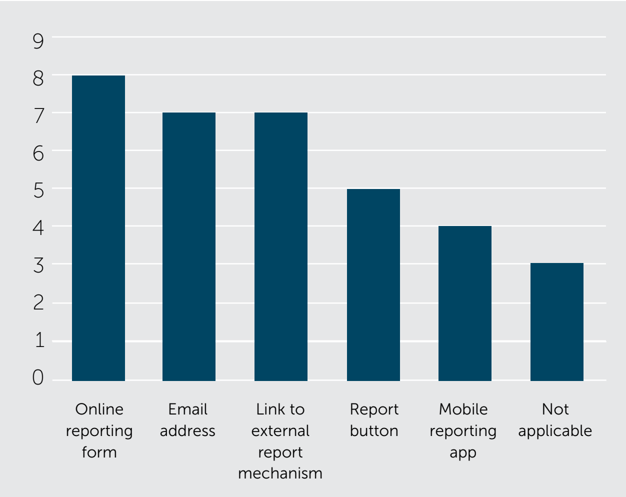
Reporting tools

Reporting mechanisms take varying forms according to the nature of the content or activity that might be reported. Reporting methods include: online submission forms, report abuse buttons, links to a safety page, an email address to report the abuse, and links to an external reporting facility such as a helpline or hotline.

Figure 3.1 gives a summary of the reporting tools available:

Figure 3.1

Reporting tools



At a minimum, most companies to which Principle 3 applies provide a report button in combination with an online reporting form to flag or report abuse. Typically located at the point where content is posted or accessed, the button opens an online reporting form or template through which users categorise the subject of the report, log its location and/or provide a free text description. An optional email address (required in the case of Deutsche Telekom) may be given in order to receive acknowledgement of receipt of a complaint.

Some companies that are connectivity-based rather than content providers (e.g. Telecom Italia, TeliaSonera) locate a reporting template on a separate safety page as the channel to report to an alert desk offending content or behaviour. As part of their safety implementation, network operators offer a dedicated email address for reporting via their customer service channels. Further, network providers typically also include a link to the national hotline or other reporting service.

More extensive reporting implementation is provided by hosting providers and content-sharing platforms (Facebook, Google, Portugal Telecom). Here reporting mechanisms and channels are central to the nature of the service and have been implemented comprehensively.

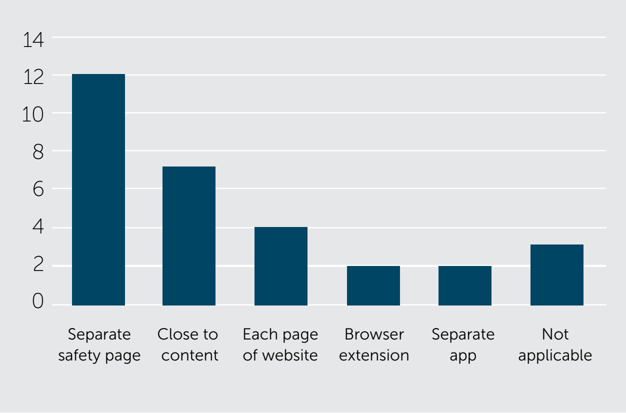
As signalled in a number of the company self-statements, a process for reporting problematic content or behaviour in the mobile environment has become an increasing priority. A number of companies have implemented (Telefónica, Orange Spain, TeliaSonera) or are in the process of rolling out (KPN, Telenor) mobile reporting apps.

Location of reporting tools

Making reporting more accessible means placing a report button or mechanism at the point where users may need it, (i.e. at every point where content is posted) or made available via a link so that users may easily recognise and identify how to report. Figure 3.2 summarises how companies have placed or located a reporting mechanism:

Figure 3.2

Location of reporting button/mechanism



All companies include a reporting facility or channel in a separate dedicated location such as a safety page. In addition, those companies offering content hosting or sharing platforms have typically provided a report button at the point where content is posted. Some also place reporting links on each page of the web service.

As noted above, reporting tools in the mobile environment are less developed. A number of companies have begun introducing a reporting mechanism via a separate app for mobile connected devices. This has been currently implemented by Telefónica, Orange and Vodafone (in Spain) and TeliaSonera, while other mobile operators plan further implementation in other markets.

Table 3.2

Who may submit reports?

Who can report?	Company
Only registered user/profile in which content is located	None
All registered users	Google TDC
Everyone including non-users	Deutsche Telekom Facebook KPN Nokia Orange Portugal Telecom Telecom Italia Teléfónica Telenor TeliaSonera Vodafone
Not Applicable	Bwin.Party LG Electronics Unibet

Who may report?

An important issue in relation to the accessibility of reporting mechanisms is the question of who may be able to report. A criticism of previous reporting solutions is that they frequently required registration on the service or platform, thus making it difficult for parents, adults or others to submit or file a report on services they may not normally use.

An open facility to report violations is an important aspect of accessibility and ensures that others who may be affected, and not just the account-holder or recipient, are able to report problematic content or behaviour. Companies were asked to confirm who is allowed to submit reports on their service. A summary is provided in Table 3.2.

The underlying approach adopted is – as stated in the submission from Nokia – that where content is visible, anyone who has access to it or with whom it has been shared should be able to submit a report. The vast majority of companies state that everyone, including non-users, is able to access a reporting mechanism. In the case of Google and TDC, however, only registered users are able to report.

Appropriate procedures for reviewing reports

Companies undertake as part of Principle 3 to implement appropriate internal procedures for reviewing reports including inter alia the provision of trained moderators to review reports. As part of the assessment, effective report handling, responsive to user needs, was discussed with ICT Coalition members. Companies confirmed that appropriate reporting handling procedures were in place, that trained moderators were available to professionally review reports and that expeditious review (both under Principle 3 and Principle 4), in accordance with the nature of the report, was a priority. Site visits to Google and Facebook included extensive discussion of report handling procedures. Some indicative evidence supplied by companies includes:

- *We have a trained team of analysts who respond and can escalate serious reports to law enforcement, NGOs and hotlines as appropriate.* (Facebook)
- *Vodafone has comprehensive customer service contact points via our retail outlets, our telephone and contact centres and online, to manage all customer issues and reports.* (Vodafone)
- *Teléfonica has its own internal channels to deal with reports received related with every kind of illegal content or misuses of its services.* (Teléfonica)
- *These measures (report reviewing) are based on effective internal processes with clear responsibilities and standard processes, which ensure that complaints are dealt with in a short timeframe.* (Deutsche Telekom)
- *The respective national abuse teams at TeliaSonera will investigate customers' report and stop the misuse.* (TeliaSonera)
- *SAPO has a call centre working from Monday to Saturday (09:00h to 23:00h). Within this period, support team receives reports, analyses them and classifies as "inappropriate" or immediately deletes the content, as appropriate. All reports are handled in less than 12h, except if received on Sunday.* (Portugal Telecom)

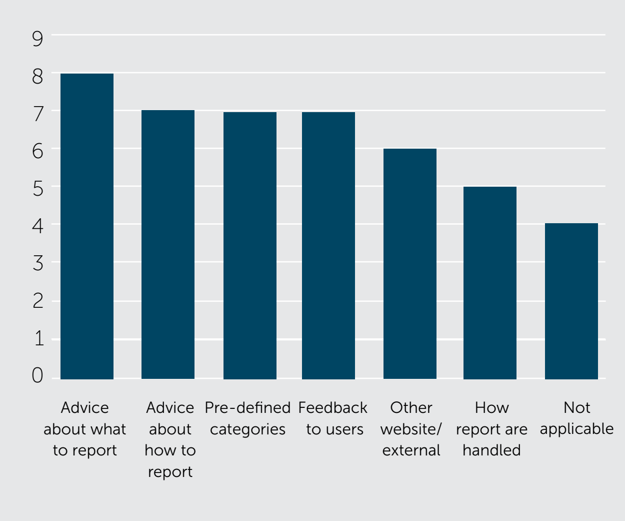
Provision of clear information to users about report procedures

Providing clear information to users about what they may report, advice about how to make a report, acknowledging receipt of complaints and providing information about how reports are handled are all features of good practice in implementing report mechanisms. As part of the ICT Principles, member companies undertake to "provide clear information to users on all available report and review procedures'".

Figure 3.3 provides a summary of the information companies provide to users in the context of making a report about abuse or misuse of its services:

Figure 3.3

Providing report information



Most companies provide information or advice on what may be reported and how to make a report (including instructions on how to use an online reporting form). Pre-defined categories are used by seven companies for reporting and as a means of handling reports. Less than half of the companies (five of the 13 to which the principle is relevant) give information about how reports are typically handled. Just six of the companies provide feedback to users on reports submitted.

Given that reporting of abuse or misuse generally involves matters of serious concern to users, many companies provide additional supporting information, links to external websites or helplines related to the subject matter being reported. This is considered further under Principle 6.

Other means of reporting

Some companies provide other channels for reporting abuse or misuse alongside or as an alternative to the use of a reporting button. Such channels can be especially important for parents, teachers and carers, who may not be registered users but may wish to report concerns or evidence of potential misuse.

Some examples of additional reporting modes presented by companies include:

- Facebook provides the possibility for anyone to report even if they don't have an account on Facebook. Accessing the desktop help page provides a link for any internet user to file a complaint about content found on Facebook or misuse of an account – such as hacking, underage use, impersonation or threatening behaviour. A complainant who is not a Facebook account-holder is asked to supply an email address when submitting their report.

- Google's Policy and Safety Hub includes additional reporting options for users, including privacy complaints as well as copyright infringement. In the case of complaints about content, reports are filed at the point where content is placed and users need to be registered to submit a report. Other reporting options include requests by family members for removal of content in cases of death or critical injury, legal reporting of defamation, trademark or copyright infringement, and privacy complaints. Complainants in this instance do not need to be registered users.

- Portugal Telecom has a Customer Ombudsman to independently assess complaints about any of it services. An online report form as well as postal and email contacts are provided.

- Telefónica Spain in collaboration with Orange, Vodafone and the national hotline Protégeles has developed an app for smartphones and tablets for reporting abuse, and harmful or illegal content.

Summary

Reporting mechanisms are a cornerstone of a safer internet environment. The commitment in Principle 3 to provide a simple and clear process whereby users can report potentially harmful content is an essential element of companies' support for internet safety.

- All but three of the companies in the ICT Coalition have implemented reporting tools, mechanisms and procedures. Principle 3 is not relevant to three companies (LG Electronics, Bwin.Party and Unibet).
- The scope of company policy on reporting abuse or misuse provides for any content or misuse to be reported. Companies in their policy statements emphasise those aspects which are most relevant to their service: content or contact that is illegal (all), content that breaches terms of service or community guidelines (user-generated content, cloud storage), or general misuse of services where no user-generated content is involved.
- All companies, with the exception of those for whom the Principle is not relevant, were found to have implemented a comprehensive range of reporting tools and options. These principally involve reporting buttons or online report forms. Most companies also provide a reporting channel via their customer help or support page.
- Reporting is typically done at the point where content is posted or visible. Other complaints such as user harassment, other threatening behaviour, privacy infringement or misuse of content may also be reported on a separate page or reporting form. Importantly, among the companies surveyed, all users and not just registered users of a service are able to make a report.
- The development of dedicated apps for reporting abuse in the mobile environment is of increasing relevance to companies and further implementations and rollouts are planned.

Overview of selected features: Principle 3

	Manufacturers/ content providers		Network/ connectivity providers				Who can report?		Report feedback
Company	Report button	Other eg. customer care	Report button	Customer care	Mobile app	External report link	Everyone	Registered users	
Bwin.Party	🟩	🟩							
Deutsche Telekom			🟩				🟩		🟩
Facebook	🟩						🟩		🟩
Google	🟩							🟩	🟩
KPN					🟩	🟩	🟩		
LG Electronics									
Nokia	🟩	🟩					🟩		
Orange			🟩	🟩	🟩	🟩	🟩		🟩
Portugal Telecom	🟩	🟩	🟩	🟩		🟩	🟩		
TDC				🟩		🟩		🟩	
Telecom Italia			🟩	🟩			🟩		🟩
Telefónica				🟩	🟩	🟩	🟩		🟩
Telenor				🟩		🟩	🟩		
TeliaSonera			🟩	🟩	🟩	🟩	🟩		
Unibet	🟩	🟩							
Vodafone			🟩	🟩	🟩	🟩	🟩		

Note: categories refer to implementation at the group level and may not be available in all markets. See individual company reports for details.

Child Sexual Abuse Content or Illegal Contact

At a glance +

Signatories shall:

- Cooperate with law enforcement authorities and other agencies, as provided for in local law, regarding child sexual abuse content or unlawful contact;
- Facilitate the notification of suspected child sexual abuse content to the appropriate law enforcement channels, in accordance with existing laws and data protection rules;
- Ensure the prompt removal of illegal child sexual abuse content once notified by national law enforcement agency;
- Provide relevant additional information and/or links to users so they can make a report or obtain information about appropriate agencies or organisations that users can contact about making a report or obtaining expert advice, at national and EU level. This could include: Law enforcement agencies; National INHOPE hotlines; Emergency services.

The sexual abuse of children in cyberspace is universally condemned as a particularly heinous crime, is outlawed in most jurisdictions and is a matter of serious concern for law enforcement. Combatting the distribution of child abuse material over the internet has been a priority for governments, policy makers and industry for the last two decades ever since international action was first taken to halt the spread of online child abuse.

Tackling illegal online content is supported internationally by the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography to the UN Convention on the Rights of the Child[1], the Council of Europe Convention on Cybercrime[2] and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[3]. The EU/US sponsored initiative on a Global Alliance against Child Sexual Abuse Online brings together 52 countries to focus action on enhancing efforts of prosecution, victim support, increasing awareness about the risks and reducing availability of child abuse material online[4].

The European Commission's Communication on European Strategy for a Better Internet for Children[5] has set fighting against child sexual abuse and child sexual exploitation as one of its four key goals. The strategy calls on industry to support efforts, including proactive measures, to remove child sexual abuse material from the internet and to increase the effectiveness of the identification of child sex abuse images, of notice and takedown procedures, and of the prevention of re-uploading.

Industry has been at the fore in such international efforts. It led, with child welfare organisations, the establishment of the first reporting hotlines in the mid 1990s. The GSMA Mobile Alliance against Child Sexual Abuse Content is one of a number of industry alliances that works collectively on obstructing the use of the mobile environment by individuals or organisations wishing to consume or profit from child sexual abuse content[6].

[1] http://www.unicef.org/protection/57929_58013.html

[2] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[3] http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm

[4] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/index_en.htm

[5] https://ec.europa.eu/digital-agenda/node/286

[6] http://www.gsma.com/publicpolicy/myouth/mobiles-contribution-to-child-protection/mobile-alliance

Under Principle 4 of the ICT Coalition Principles, signatories undertake to cooperate with law enforcement authorities and other agencies, to facilitate the notification of suspected child sexual abuse content to the appropriate channels, in accordance with existing laws and data protection rules, and to ensure the prompt removal of illegal child sexual abuse content once notified by a national law enforcement agency. National legislation determines the specific requirements for processing reports and procedures for removal of content once notified. ICT Coalition members undertake to support all necessary actions as provided for in national law. Furthermore, companies undertake to support additional-awareness among their users regarding online child sexual abuse as an issue, and about how to make a report, and to provide links to relevant support and law enforcement agencies.

Scope of company policy

The E-commerce Directive 2000/31/EC provides the legal basis for exemption from liability for online service providers in Europe for content that they host on condition that they do not have "actual knowledge" of illegal activity and that, on obtaining due notification, they act expeditiously to remove or disable access to such material. This forms the basis of "notice and takedown" procedures. In addition, Directive 2011/92/EU on combatting sexual abuse and sexual exploitation of children and child pornography provides for the prompt removal of websites containing or disseminating child-abuse material hosted in a members state's territory. In addition, member states may block access to such webpages in accordance with transparent procedures and adequate safeguards.

Companies in the ICT Coalition confirm a zero-tolerance policy towards use of their services for distribution of children abuse material and under Principle 4 undertake to implement measures to combat illegal online content.

In their self-statements and implementation reports, companies outline the key features of their policies on combatting online child abuse. Policies comprise:

- Statements that outline how child sexual abuse and illegal content or conduct are prohibited in the respective terms and conditions of the service
- Reinforcement of terms and conditions in user or community guidelines applied to the service
- Implementation of reporting mechanisms or links to national hotlines for reporting suspected child abuse material
- External partnerships and affiliation with relevant national and international organisations, including law enforcement agencies dedicated to fighting online child abuse
- Procedures for implementing 'Notice and Take-Down' processes to enable the removal of any child sexual abuse content posted on their own services
- Company measures – where applicable - to proactively detect and combat the spread of child abuse material.

A number of ICT Coalition members are founder members also of the GSMA's Mobile Alliance Against Child Sexual Abuse Content[7] which works to prevent the use of the mobile environment by individuals or organisations wishing to consume or profit from child sexual abuse content.

Three companies (Unibet, Bwin.Party and LG Electronics) cite that Principle 4 is not applicable to their products or services. Each, however, also deploys policies to counter online child abuse. For example, LG Electronics declares that "in the unlikely event that its Smartworld online store was compromised, its monitoring and pre-approval process has the capacity to counter the breach and notify relevant authorities". Similarly, while it does not directly host user-generated content, Unibet argues that its international customer services team has the ability to report feedback, issues or complaints concerning any violation of its service terms.

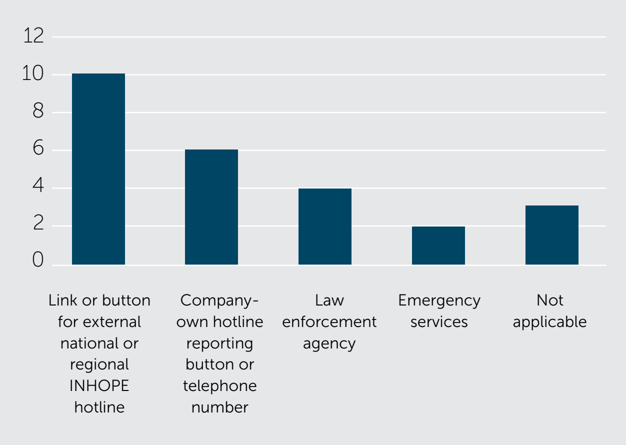
[7] Deutsche Telekom, Orange Group, Telecom Italia, Teléfonica Group, Telenor Group, TeliaSonera Group, Vodafone Group

Reporting mechanisms for child abuse

Companies were asked to identify the mechanisms provided in their products or services to facilitate the notification or reporting of child abuse content. Figure 4.1 summarises the responses:

Figure 4.1

Reporting mechanisms for suspected child abuse content



A link or reporting button that links to the national hotline or INHOPE member is the main mechanism deployed by most companies as a means of notifying or reporting suspected child-abuse content. Of the 13 companies that provide such a mechanism, 10 provide a link to the national hotline. In the case of five companies (Deutsche Telekom, Facebook, Google, KPN, TeliaSonera) this is the preferred approach and takes the place of an own-company reporting mechanism. In the case of Orange, Portugal Telecom, Telefónica and Vodafone, there is both an own-company reporting channel and a link to the national hotline reporting facility. Nokia, by virtue of the nature of its international service, processes any notices of child-abuse material through its 'report abuse' option.

A number of companies include or prioritise direct liaison with law enforcement in the reporting of abuse. Orange and Facebook also state that that they involve emergency services where appropriate when notices are received.

Procedures used

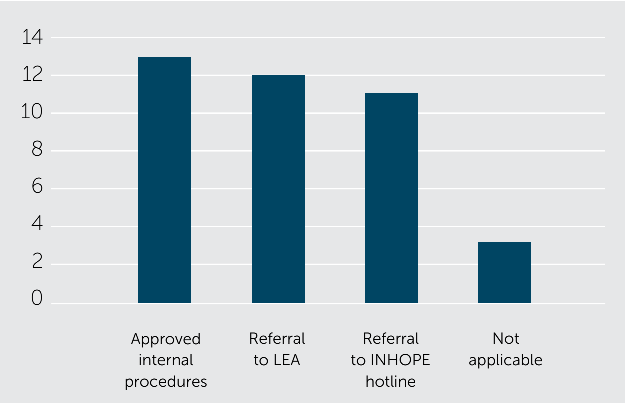
Companies were asked to outline briefly the procedures to be followed if illegal content were to be discovered on their service. The precise steps vary from country to country, depending on applicable local laws, though many of the companies have adopted the framework outlined by GSMA's notice and take down procedure[8] which, in summary, identifies the following main steps:

1. A complaint is made through customer care
2. It is assessed for potential illegal content and referred to Fraud and Security
3. If confirmed as potentially illegal, content is removed from public view and passed to appropriate authorities for assessment
4. Depending on national laws, content is removed and provided in evidence to the appropriate authorities.

A summary of responses provided by companies is presented in Figure 4.2.

Figure 4.2

Report handling procedures



[8] http://www.gsma.com/publicpolicy/wp-content/uploads/2012/07/Mobilecontributiontonoticeandtakedown.pdf

Ten companies overall include the above distinct steps in their report handling procedures. These include an approved internal procedure for handling reports, referral to law enforcement agencies and/or referral to the INHOPE hotline. The precise sequencing and combination of these steps varies according to the market concerned. There are, for instance, notable variations across European countries in the handling of suspected illegal content, which in some countries can only be assessed by law enforcement agencies or removed only on instruction from the judiciary or law enforcement. KPN, for instance, observes that the handling of any child abuse content is strictly illegal and accordingly all reports are forwarded to the national hotline for processing. Portugal Telecom, by contrast, declares that manifestly illegal content proactively identified by its team is immediately removed.

External links and relationships

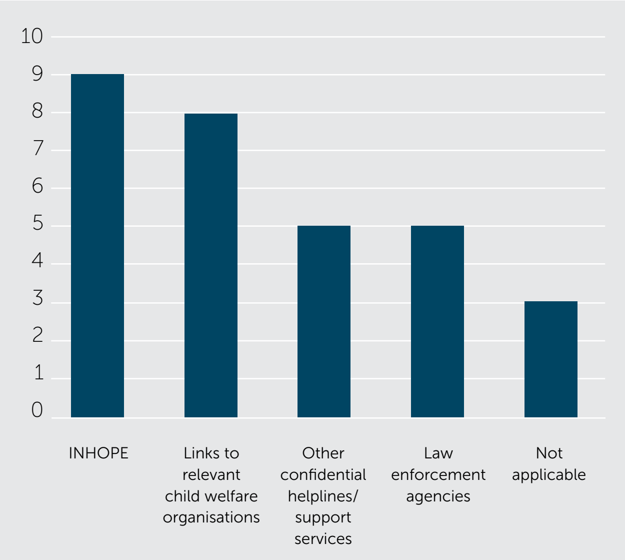
Companies, as part of their overall approach towards combatting online child abuse, have formed a range of partnerships and links with relevant external agencies and organisations. In the case of processing and onward forwarding of reports of suspected illegal content, close working relationships are required with the relevant national hotline and law enforcement agencies in each country. For companies that operate in different European markets, therefore, there is an additional responsibility to develop and adopt different policies and procedures as well as to negotiate the necessary relationships with relevant agencies in each country.

Alongside this, many companies also maintain links with external helplines, support services or other specialised agencies dealing with child welfare. For example, TDC has, jointly with other ISPs and telecommunication operators and with the Danish police department for IT crimes (NITES), developed an agreed procedure for handling child sexual-abuse content. This includes guidelines to ensure that the ISPs are constantly updated with lists of relevant IP addresses from the police. The police monitor traffic accessing addresses containing child-abuse content. These are then blocked by ISPs while police via Interpol – if relevant – investigates hosts and sources.

A sample of the kinds of relationships that companies have developed is shown in Figure 4.3

Figure 4.3

Links ro external agencies



Additional measures

A number of companies have introduced additional measures to combat child abuse content alongside formal requirements to implement notice and take-down procedures as specified by local or national laws.

Mobile operators, for example, under the terms of the GSMA Mobile Alliance, are working towards implementation of the Internet Watch Foundation (IWF) blocklist in national markets where this is legally permissible. Among ICT Coalition members, the Orange Group, Telefónica in Spain and the UK, and Vodafone block access to illegal URLs as defined by the IWF where legal to do so.

Similarly, TeliaSonera, working with the software provider Netclean, provides a whitebox solution called 'Child SafeGuard', to block child sexual abuse material at the IP-level in cooperation with the Internet Watch Foundation. Child SafeGuard is placed in

TeliaSonera's IP transit network in Sweden and Spain. TeliaSonera is also seeking to implement blocking of child sexual abuse images in additional countries.

Other examples of proactive measures introduced by companies include the following:

- Deutsche Telekom uses contractual agreements which require third-party content providers or partners with which there are commercial relationships to follow equivalent notice and takedown rules.
- Facebook applies PhotoDNA to prevent upload of child abuse images and runs NCMEC and Facebook's own hashlist on all images uploaded. It has also created a direct escalation channel with relevant networks (INHOPE, Insafe, ECPAT) for more effective notification.
- Google has introduced a range of measures in a global strategy on combatting child online exploitation including investment in technology, hardware, software and use of 'hashing' technology to tag known child abuse images. As of December 2013, Google now shows warnings – from both Google and charities – at the top of search results for more than 13,000 queries. These alerts make clear that child sexual abuse is illegal and offer advice on where to get help. Google also recently announced a $2m Child Protection Technology Fund to encourage the development of more effective tools.
- For Microsoft services accessible through Nokia Lumia devices, Nokia relies on Microsoft to handle takedown of child abuse materials, including, for example, materials uploaded to SkyDrive.

Summary

The process of combatting online child abuse material is long-standing among members of the ICT Coalition.

Notice and take-down procedures provide the principal basis on which this is achieved; there are well-established protocols on removing content based on notification by competent authorities within each jurisdiction. Hosting providers, platforms for user-generated content and mobile connectivity providers, adopt broadly similar approaches. Proactive measures to detect and remove child abuse material have also been adopted by a number of companies.

- All companies in the ICT Coalition have implemented policies to combat online child abuse. The scope of company policy includes definition on their respective services of prohibited content or conduct that is illegal.
- Three companies - LG Electronics, Unibet and Bwin.Party - declare that Principle 4 is not relevant to their product or service.
- Each of the companies for which this Principle is relevant have implemented mechanisms to facilitate the notification of suspected child abuse content comprising a combination of reporting channels provided by companies as well as links to the national hotline (or INHOPE) for the reporting of online child sexual abuse.
- Report handling procedures in accordance with national law have been implemented in each of the companies concerned.
- Companies provide, in addition to links to relevant law enforcement agencies and national hotlines, a range of informational resources and additional links to external organisations providing information and support in relation to child abuse.
- A range of proactive measures are also supported including the blocking of known child abuse material, technical measures to detect and to prevent the uploading of child abuse content, and investment in new technical tools to combat its wider dissemination.
- As described by mobile connectivity companies, a more consistent and streamlined approach across European markets would provide a more effective approach to notice and takedown. Currently, operators have established different approaches, policies and relationships with relevant authorities in each of the markets in which they operate.

Overview of selected features: Principle 4

Company	Company-own hotline reporting button or telephone	Link or button for external national or regional INHOPE hotline	Emergency services	Law enforcement agency	Links to relevant child welfare organisations/ specialist providers of advice	Other confidential helplines/ support services	Other agency
Bwin.Party							
Deutsche Telekom		🟩					
Facebook		🟩	🟩	🟩	🟩	🟩	🟩
Google		🟩			🟩		🟩
KPN		🟩					
LG Electronics							
Nokia	🟩						
Orange	🟩	🟩	🟩		🟩	🟩	
Portugal Telecom	🟩	🟩			🟩	🟩	
TDC				🟩	🟩		
Telecom Italia	🟩						
Telefónica	🟩	🟩			🟩	🟩	
Telenor		🟩		🟩	🟩	🟩	
TeliaSonera		🟩					
Unibet							
Vodafone	🟩	🟩					🟩

Note: categories refer to implementation at the group level and may not be available in all markets. See individual company reports for details.

Privacy and Control

At a glance +

Signatories should:

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

Protecting users' privacy and personal data is now a topic of enormous importance for the entire internet industry. Against a background of intense sensitivity regarding the security of personal data, companies have been at pains to reassure the public of the integrity of their systems and to reinforce trust and confidence that their personal information is safe. At the same time, EU law places a high premium on data privacy as a fundamental right and allows the collection of personal data only for legitimate purposes under strict conditions. Technology, telecommunications and internet service providers thus have extensive experience of data protection, in an environment where strict regulation applies.

From the perspective of child online safety, somewhat different issues arise. Children and young people's online interactions may lead them to share more personal information than intended, whether due to insufficient experience, a lack of digital literacy skills or immaturity in relation to decisions about sharing personal data. Through their use of social media, sharing of content or online communications, children may reveal personal information that may make them vulnerable to unwanted or harmful contact or might damage their reputation in some way. Children's exposure to commercial messages and direct marketing is a further topic of increasing concern; with children going online at a younger age, this is something that researchers and child-welfare specialists have increasingly called attention to.

Industry providers have been called upon to ensure that their services incorporate age-appropriate privacy settings to enable young people as well as parents to make informed decisions about their management of personal information. It is recognised that the default settings for online services have an important bearing on how such services are subsequently used and deployed; accordingly there have been many calls for providers to implement a level of 'privacy by default' that ensures young people are as safe as possible.

Members of the ICT Coalition have given a commitment to implement privacy settings that are appropriate to the age of the user and that ensure young people's safety. Companies undertake to offer privacy options and settings that are accessible, easy to use and understand, and empower users and their parents to maintain control over information they share online. Further, companies commit to raise awareness among users as well as the wider community about effective use of privacy controls and of good practice in this regard.

In addition to company self-statements about their commitment to age-appropriate privacy settings, for the purposes of this assessment companies were asked to supply details of the scope of their company policy on privacy as related to minors, and the application where relevant of distinct privacy settings for young people under the age of 18. Companies were also asked to demonstrate how they supported education and awareness-raising on the subject of privacy.

Scope of company policy

Companies' privacy policies as relevant to Principle 5, summarised below, outline the main features of how each company defines its position on privacy (as relevant to their service) and the context in which it operates according to European data protection legislation. As the companies involved offer diverse products and services, the company policies of manufacturers, connectivity providers, and content and service providers are discussed in turn.

Manufacturers

Manufacturers' contribution to good privacy practice in relation to child online safety stems mainly from issues of design and to ensuring insofar as possible that applications developed for their products comply with regulatory requirements and offer reasonable protection. For the purposes of Principle 5, LG Electronics, Nokia and Google are manufacturers of hardware products and devices that can be used for internet access, online interaction and content-sharing.

- LG Electronics states that, while its products are not made for children, it has taken actions in order to raise parental awareness of privacy-related issues and that it encourages parents to educate their children when using the internet on LGE's products. There is no age restriction on use of LGE's products or services. It has, as of 2013, introduced a third-party parental control product on its new mobile phones (see Principle 2).
- Nokia sets 13 as the minimum age for the use of its products and services. It does not design or market its products or services for children. Company policy states that it encourages parents to register on behalf of any children under 13 years of age. For minors aged over 13, registration is subject to legal competence under local law. Its products and services are typically intended for general audiences. Nokia states that it does not knowingly collect information about children without the consent of their parents or guardians.
- Google, in addition to its range of internet services, offers a number of hardware products, including smartphones, notebooks and tablet devices that may be used by children and young people. These primarily use the Android mobile operating system. Company policy states that appropriate settings are provided to enable users to control the data they share. This includes the ability to control access to location data when using mobile versions of Android or Chrome OS. Android 4.3 also features 'Restricted Profiles' (see Principle 2) that limit the access that others have to features and content on the tablet or mobile device.

Connectivity and network operators

Ten of the companies in the ICT Coalition are network or telecommunications operators offering a range of services for fixed-line and mobile connectivity services. As such, their operation and access to customer data is regulated under strict data protection law. Similarly, any IPTV services offered do not allow for sharing of personal data.

The principal privacy issues that arise are those concerning the use of applications or services, particularly in the mobile environment, on the networks operated by these companies. In this context, many of the companies involved cite in their submissions adherence to the GSMA's Mobile Privacy Principles[9] and have implemented, or are in the process of, implementing the Privacy Design Guidelines for Mobile Application Development[10]. These guidelines are intended to support a more consistent approach to user privacy across mobile platforms, applications and devices. They establish privacy rules, for example for social networking and social media apps, or applications including mobile advertising. With respect

[9] http://www.gsma.com/publicpolicy/mobile-and-privacy

[10] http://www.gsma.com/publicpolicy/mobile-and-privacy/design-guidelines

to children and young people, the principles recommend, inter alia, that applications be tailored to appropriate age ranges and to have location default settings that prevent users from automatically publishing their precise location.

- Deutsche Telekom states that given the limited applicability of Principle 5 to its services, its focus is on implementing the GSMA Privacy Design Guidelines for Mobile Application Development which it will introduce in each of its subsidiaries.
- KPN offers a range of fixed and mobile telephony, internet and TV services under national data protection and telecommunications legislation. Its child-oriented MyBee browser application has a separately published privacy policy.
- A signatory of the GSMA Privacy Guidelines for Mobile Application Development, Orange has developed internal guidelines intended for product managers, available as of January 2014, together with a best practices implementation guide, giving step-by-step advice to product managers and developers. The Orange Group signed in 2013 a charter highlighting the group's commitment to protecting customers' privacy and personal data.
- Portugal Telecom's privacy policy does not specifically address minors but in relevant terms of use for its services highlights where there are specific recommendations to minors.
- Telecom Italia requires parental consent in the use of mobile services such as TIM Young, TIM cinema, etc. The TIM Young service has specific measures for protection of minors, such as a blacklist of sites and content that minors cannot access and the blocking of minors' personal data for marketing and profiling purposes.
- Telenor has fully implemented the GSMA Privacy by Design Guidelines, providing minimum standards for application development in order to safeguard the privacy of users. Telenor has no own-branded apps directed at children or adolescents at present. Any own branded apps are for the purposes of managing subscriptions and monitoring consumption (so-called 'utility apps'). These are stated to be offered in compliance with the privacy policy of each business unit offering the app, published on the individual company websites.
- Vodafone does not offer a social networking service or in-house app store. However, it has existing policies and a code of conduct that would require it to provide separate default privacy settings for younger users. It states that it does not actively identify children for marketing purposes and that any known children's data is flagged and excluded from marketing campaigns.

Content and service providers

Five companies in the ICT Coalition offer content sharing services that are relevant to the Principle 5 commitment to offer age-appropriate privacy settings. In relation to the scope of company policy as outlined in the relevant section of their service:

- Bwin.Party declares that all points of its privacy policy refer only to data of 18+ users. Data usage is also restricted; "personal information is collected for no other purpose than that related to the operation of the Services". There is thus no disclosure of information to other users or third parties that is not directly linked to the functioning of its gambling product.
- Unibet similarly does not allow under-18s to access its services and thus does not collect data or allow data sharing of minors.
- Portugal Telecom on its portal and collection of content services (SAPO.pt) highlights in bold text relevant sections of privacy policies directed at young people.
- Facebook's Data Use Policy provides a comprehensive and user-friendly guide to how user information is collected and processed on Facebook services. It explains the application of privacy settings, sharing of information with third-party apps and games, advertising and user profiling, as well as the use of cookies and other technologies. It also provides a link to a dedicated resource on 'Minors and Safety' from a data use perspective.
- Google specifies both in its data-use policy and in the submissions to the ICT Coalition the range of settings provided to manage sharing of personal data. This covers a diverse range of services (see below) and includes communication, content-sharing, browsing, and search and operating system software.

Privacy settings for under-18s

A key feature of companies' implementation under Principle 5 is the provision of privacy setting options that are easy to understand, prominently placed, user-friendly and accessible, and which encourage users – parents as well as children and young people – to make informed decisions about their use of the service and the information they post and share with others online.

Companies were asked to supply information about the privacy options available and, specifically, if distinct privacy settings were deployed to prevent access to personal data for users under the age of 18. Nine of the companies deemed this not applicable while seven provided details of the under-18s privacy controls relevant to their services.

Table 5.1

Under-18s privacy settings

Under-18s privacy settings	Company
Not applicable	Bwin.Party Deutsche Telekom LG Electronics Orange TDC TeliaSonera Unibet Vodafone
Available settings for under-18s	Facebook Google KPN Nokia Portugal Telecom Telefónica Telenor Telecom Italia

Privacy settings offered by connectivity providers take account of minors' privacy protection in the following ways:

- Telefónica Germany provides prepaid mobile phone services for customers from age 16 that are optimised for teenagers. In the UK, Telefónica via O2 prohibits collection of data from under-16s for marketing purposes.
- Telenor Norway has a 'Safe Child package' for mobile subscriptions that prevents information about the user from being published in phone directories.
- KPN offers a free downloadable browser for children, MyBee, whose browsing capabilities are restricted and within which only parent-approved content is offered. A mobile version for iOS is also available.
- Portugal Telecom's SAPO Mail Kids (age 6-13) is an email service in which adults set the rules for sending and receiving e-mails, including the creation of a list of authorised contacts. Similarly, its MEO Kids mobile subscription plan allows only 15 contact numbers as defined by parents while also barring premium or value-added services.
- Telecom Italia's policy guidelines on compliance requirements for mobile apps includes provision for minors' privacy protection, prohibiting their profiling - direct or indirect - for commercial purposes and the collection of geo-location information.

The submission by Google details privacy settings deployed for under-18s on its services, the main features of which include:

- Minimum age requirements (13 or older in most countries; 14 in Spain; 16 in the Netherlands) to own an account in accordance with national provisions. Some of its services (for example, Google Wallet, or restricted video content on YouTube) are only available to over-18s.
- Default settings for the Google+ platform for teens' accounts limit communication to the people in 'your circles' (for 18+, the default is 'Anyone'), i.e., they won't see comments from people outside their circles on their public posts, and those people can't contact them via Google+. Contact is restricted for those outside a teen account's circle, including in hangouts. Personal information including contact details and birthdate are restricted to 'only you'. Location information is disabled by default. Finally, changing default settings for a post's audience brings up a reminder to encourage teenagers to think before they post.

- YouTube includes a range of customisable settings that affect how content is shared. 'Safety Mode' may be locked to provide safer internet viewing. Comments may be moderated, edited or blocked as required in the settings option. Video posting by default is set to 'public' but may be changed in privacy settings to 'private' or 'unlisted'.

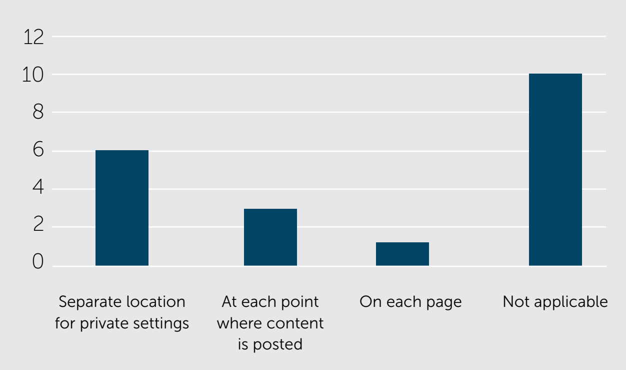
Facebook's submission in relation to default settings for privacy includes the following key features:

- Facebook sets 13 as the minimum age for the use of its social network.
- Facebook provides enhanced privacy for minors' accounts (age 13-17). New users are automatically defaulted to share with 'friends' only. Minors are reminded who they are sharing with and, if they share publicly, receive specific educational messages about what it means to post publicly.
- Minors cannot receive messages from strangers. Personal, sensitive information including minors' contact information, school or birthday is not available to a public audience.
- Minors' accounts do not have listings created for them in search engines. Their ability to share their location is automatically defaulted to "off".
- Minors can only be 'tagged' on Facebook by a maximum of their friends of friends.

Companies were also asked to identify the location of privacy settings where users may view, change or update their privacy status. An overview of relevant provision of privacy settings is as follows:

Figure 5.1

Location of privacy settings



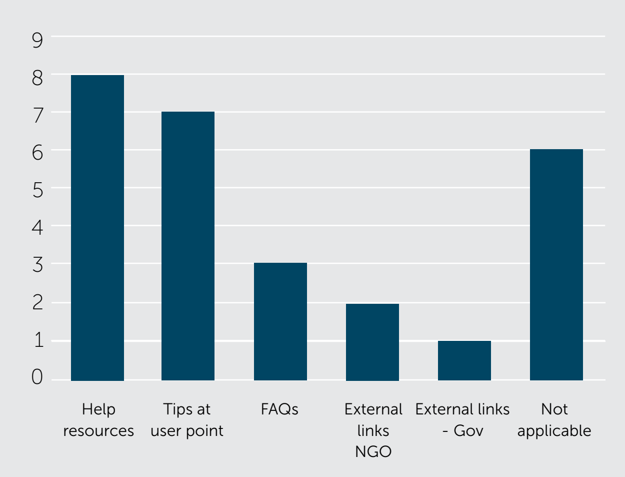
such as a privacy page or tab linked to the service. In the case of content sharing platforms, Facebook, Google and Portugal Telecom each provides opportunities to view and change privacy settings at each point where content is posted. Facebook, in addition, provides a link to privacy options across each page of the service as well as an activity log at which it is possible to revise privacy settings for historical postings.

Resources and help features related to privacy

Part of the commitment to support better privacy and control for younger users is the provision of education and awareness-raising about privacy, how to manage it and to reinforce good practice with appropriate educational material. Companies were asked to outline what information, resources and help features (if any) they provided to encourage users to make informed decisions about their privacy or the information they share.

Figure 5.2

Availability of information, resources or help features



Companies mostly provide online help resources incorporating more detailed explanations of privacy features, such as videos and tutorials about how to use and manage privacy settings. This is supplemented, in particular by companies offering content sharing platforms, with tips and reminders at points in the service where users post content, send messages and make friend contacts. External links to NGOs are mentioned just by Google and Portugal Telecom and only the latter provides links to a government agency, e.g. in relation to data protection.

Noteworthy additional features related to privacy protection as well as education identified during the assessment include the following:

- Telefónica (Spain, German, UK) provides useful video tutorials explaining privacy policy in an accessible, easy-to-understand way.
- Vodafone's animation on its corporate website, 'Privacy by design across the mobile ecosystem', is also a model of clarity in explaining the complex interdependencies in privacy regulation and protection from a global perspective[11].
- Google provides a valuable glossary of key terms in its resources on 'Policies and Principles' providing at least for parents a user-friendly explanation of technical aspects of data collection, retention and sharing.
- Google also provides a facility in YouTube for parents and legal guardians to submit a privacy complaint if they feel their child's privacy has been violated in some way.
- Facebook also report that it has industry-standard and proprietary network monitoring tools running on its system in order to prevent security breaches that might threaten the security of users' data. This includes posting to a secure page when logging in which uses industry-standard encryption to ensure all logins are secure.

[11] http://www.vodafone.com/content/index/about/about-us/privacy/privacy_by_design.html

Summary

Privacy protection has become a highly sensitive topic. Companies have responded in a number of ways to instil user trust and confidence in the security of their products and services when sharing or processing data.

The interdependence of different parts of the internet eco-system makes privacy quite a complex undertaking, which relies on each actor supporting privacy protection features. Concerning child online safety, all companies have agreed as a minimum to make available age-appropriate privacy settings and to offer accessible and easy-to-follow supporting information and advice about privacy matters for those using their services.

- Manufacturers support better privacy and control under Principle 5 by including privacy-enhancing design features such as built-in parental controls to provide additional protection when products are used by younger children.
- Connectivity providers have, through initiatives such as the GSMA's Mobile Privacy Initiative, sought to build privacy considerations across platforms, applications and devices. Specific protections for children and minors such as limiting geo-location settings and privacy rules for social networking and social media apps, are examples of good practice. Implementation of the GMSA privacy guidelines has been a valuable addition to protecting young people in the mobile environment.
- Content and service providers such as Facebook, Google and Portugal Telecom have incorporated a range of privacy options to give users control over what they post and how they share content. The settings and facilities provided are comprehensive and are easy to use, and provide a crucial ingredient in an overall framework for safer internet use by young people.
- Default settings for minors vary according to the nature of the services involved; while there is no single approach, companies have made efforts to provide a range of options for new users that establish a good foundation for better privacy management and control.
- Resources and awareness-raising materials provided by companies with platforms for content-sharing are comprehensive and are a valuable contribution to educating users on privacy protection.

Overview of selected features: Principle 5

	Privacy settings	Location			Other features / resources			
Company	Privacy settings for under-18s	On each page	At each point where content is posted	Separate location for privacy setting	Tips at user point	FAQs	Help resources	GSMA Privacy by Design Guidelines
Bwin.Party				🟩				
Deutsche Telekom								🟩
Facebook	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
Google	🟩		🟩	🟩	🟩	🟩	🟩	
KPN	🟩			🟩	🟩			
LG Electronics								
Nokia	🟩				🟩	🟩	🟩	
Orange							🟩	🟩
Portugal Telecom	🟩		🟩	🟩	🟩		🟩	
TDC								
Telecom Italia	🟩						🟩	🟩
Telefónica	🟩				🟩		🟩	🟩
Telenor	🟩			🟩	🟩		🟩	🟩
TeliaSonera							🟩	🟩
Unibet								
Vodafone							🟩	🟩

Note: categories refer to implementation at the group level and may not be available in all markets. See individual company reports for details.

Education and Awareness

At a glance +

Signatories should:

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

The role of education in promoting better awareness of internet safety is one of the most frequently pointed-to solutions in current policy debates. There is wide consensus across different stakeholder groups that better resilience comes from children acquiring the skills to protect themselves. But who is best equipped to provide children with such digital literacy and safety skills? In the first instance, parents may be said to have the primary responsibility for guiding children in their use of the internet and teaching them from an early age about safe and responsible use. However, parents may need support and education themselves in improving their own digital literacy skills. Schools are also uniquely positioned to reach children in ways that others may find it difficult to do, and are widely respected as a trusted source of information. Accordingly, the European Commission's Strategy for a Better Internet for Children[12] called on member states to step up its support for internet safety education and specifically to introduce teaching of internet safety in school curricula across Europe by 2013.

However, schools, just as parents, do not always have the expertise or the capacity to be the main source of internet safety guidance. In this context, the European Commission called on industry to support educational efforts through private-public partnerships and by providing educational and awareness materials for teachers and children. In practice, many companies have a long history of support for educational initiatives and promoting wider digital literacy. Companies have included educational outreach as part of their corporate social responsibility programmes. They have integrated education in product offerings, developed materials for classroom use, and contributed directly to delivery of training.

The ICT Principles include awareness-raising as an element in each of its key actions (content, parental controls, reporting and privacy). Principle 6 articulates a broader commitment to promote children's internet safety through education and awareness-raising. It requires companies to provide up-to-date information on the settings and services offered in a way that is accessible to young people and helps to keep them safe. Messaging about internet safety should be addressed to young people as well as to parents, teachers and carers in order to enable them to learn more about how to manage children's internet experience. Finally, industry is encouraged to work

[12] http://ec.europa.eu/digital-agenda/en/creating-better-internet-kids

with others in supporting quality sources of information and advice about keeping safe online, about responsible use of new communications platforms and about values of critical media literacy and digital citizenship in today's society.

Principle 6 is framed in a way that leaves scope for companies to identify priorities and support their own implementation of internet safety with appropriate informational resources. In this assessment, companies were asked to detail what activity they had undertaken in support of Principle 6: what educational resources they had developed, if any, and for which audience; what topics they had addressed, and what kinds of learning outcomes had been considered. They were also asked to detail any partnerships with educational bodies, NGOs or other industry, in support of education. Materials and resources were reviewed against the template of Principle 6 to provide an overview of the level and depth of support for education and awareness-raising among members of the ICT Coalition.

Scope of company policies

All but one of the companies in the ICT Coalition contributed information in relation to their education and awareness under Principle 6 of the ICT Principles. Unibet's self-statement declares that the Principle is not relevant to its service, but that it adheres to the Code of Conduct of the European Gaming and Betting Association, against which it is audited, and promotes safe, responsible online gaming on its services.

Company policy as reported by respondents is primarily set at the corporate level with roll out to individual local markets and/or local initiatives being developed at subsidiary level. Policy objectives and the value of educational and awareness-raising initiatives are underlined at the corporate level as part of corporate social responsibility. They also help to promote the brand and the quality of the product or service concerned.

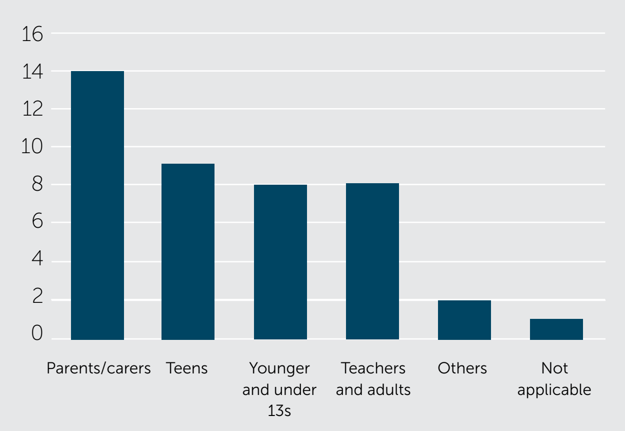
The range of initiatives and activities represented within the scope of company policy is extensive and diverse. Presentation of online resources is one of the main vehicles by which companies disseminate educational resources and materials. These are further supplemented by a range of published materials, including 'how to' and 'best practice guides' suitable for use in educational settings. Companies also include within their policies support for awareness-raising campaigns such as Safer Internet Day at a European level and local or national initiatives. Strategic alliances with NGOs, organisations with educational outreach expertise and with relevant agencies in education also feature. Companies are also active agents in delivering education and training through in-schools demonstrations and visits, seminars and workshops and internships. Finally, companies in some instances declare support for education through research initiatives, either own-company or commissioned research relevant to their product or service.

Target groups

To gauge the age range and subject of their educational approaches, companies were asked to identify which groups their educational resources were targeted at. These are summarised in Figure 6.1.

Figure 6.1

Target age groups for educational resources



Parents stand out as the most important target group of materials produced by companies, followed by teenagers, and teachers and other adults. Fewer companies, with some notable exceptions, offer resources targeted at younger users.

- For example, Vodafone states that its priority, since its launch of the first mobile parental controls in 2005, is "supporting parents to enable them to make informed decisions on advising and protecting their children online". This involves making them aware of the tools available and providing insight into views of other parents and parenting specialists on the approaches to online safety. Its Digital Parenting Initiative, launched in 2009, continues this theme.
- This approach is echoed by a number of other companies in their submissions, e.g. Orange, LGE, Nokia and TDC, which identify parents and adults as the primary customers to whom advice is directed in the first instance. Such advice mainly consists of a range of online help resources on their websites, containing advice to parents and users in general about how to ensure safe internet use as well as use of mobile phones by children. Similarly, Nokia cites its rollout of parental controls on relevant devices as an opportunity to promote 'how to' guides for parents using such devices and controls, as well as guidance on the age-ratings approach for apps or mobile content.

Teachers are also an important target group particularly in the context of partnerships that companies have supported for developing and delivering training initiatives:

- Google's Google for Education is an online resource encompassing a wide range of materials for teachers and schools, such as the Google Digital Literacy and Citizenship programme which includes lesson plans and educational materials. The handbook *The Web We Want,* aimed at 13-16 year-olds, is a notable example of partnership (with European Schoolnet and supported by Liberty Global); it fills an important gap in providing relevant, up to date curriculum materials for schools as they struggle to keep pace with demands for greater attention to internet safety education.
- TDC together with other operators in Denmark via the National Telecom Industry association (TI) as well as with NGOs such as Children's Welfare and Save the Children, has developed materials both online and in the form of workshops for teachers that aim at increasing awareness among pupils on the safe and responsible use of the internet and social media.
- Facebook includes a variety of materials for teachers, with dedicated resources and tips in the Family Safety Centre targeted at teachers, such as its Facebook Guide for Educators and Community Leaders handbook promoting safety, privacy and digital literacy. A poster encouraging young people to think before they post and a handbook for school counsellors is also included. A version for the UK, produced in association with The Education Foundation, acts as a guide for teachers on the use of Facebook in the classroom as a tool for digital and social learning, as well as an introduction to safety features available on Facebook.

Content-sharing platforms and services used by children provide the main contexts in which education and awareness materials are likely to be targeted at young people as end users. Examples are:

- In Germany, Telekom Deutschland operates a 'kids portal' (kids.t-online.de), providing safe, positive content for children. Categories include games, politics, information resources, knowledge, entertainment to name but a few, as well as the search engine for kids, *fragFinn.de,* which offers a safe surfing environment for children within a protected online space. A fragFINN app, available since 2012, offers a child-friendly browser for smartphones and tablets.
- A related example presented by Google, also in Germany, is the *juki* project – combining video community, interactive lessons, an encyclopaedia and an animation *studio. juki.de* forms part of the German government's initiative Ein Netz für Kinder (A Net for Children) and is supported by the Federal Ministry for Families and Youth and the Federal Ministry for Culture and Media. Other partners include the German child welfare association DKHW, and voluntary self-regulation organisations FSF and FSM.
- A further example, also presented by Google, is a recent special edition of the Donald Duck magazine in Norway which focuses on internet safety using familiar children's characters and stories to develop messages around digital skills and online safety.
- Vodafone similarly developed its Digital Facts of Life 'Web Super Skills' Moshi Monster cards launched in Ireland, Spain and UK in November 2013. Aimed at parents with children aged 4-8, the purpose of the pack is to act as a discussion starter, with simple messages for parents to talk to their children about. The cards are available to Vodafone customers and as a downloadable pack for schools.

Topics covered

Given the extensive volume of materials, a wide range of topics is covered. The main areas of risk addressed, as identified in implementation reports, are issues of cyberbullying, illegal downloading, and contact with strangers. Figure 6.2 summarises the responses from companies.

As Figure 6.2 highlights, nearly all companies include general tips and advice on safe online behaviour as well as guidance on safe mobile use supplied by mobile connectivity companies. Figure 6.3 gives an overview of the main methods and formats adopted.

Figure 6.2

Topics covered in educational materials

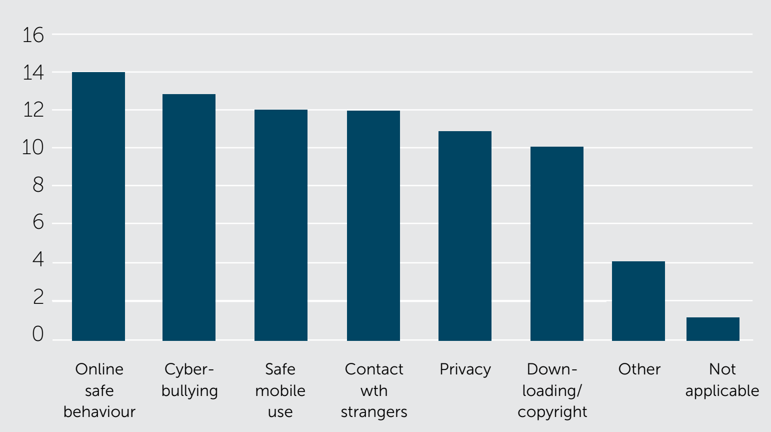
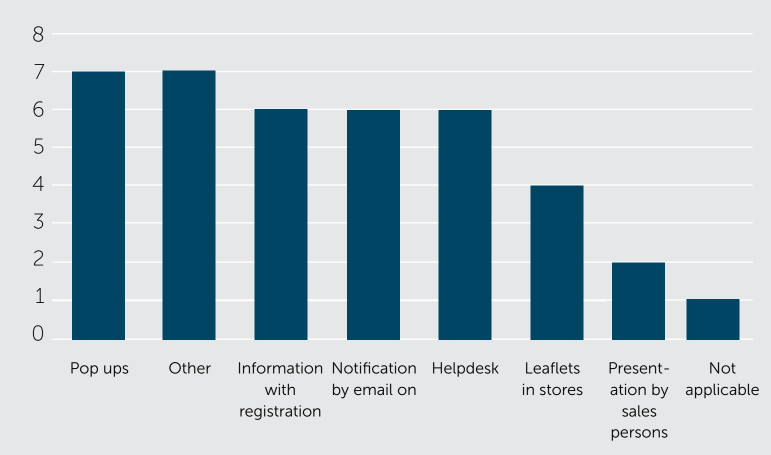


Figure 6.3

Format of education material



Another important format for educational activity supported by companies not directly represented above is that of active participation in campaigns and initiatives related to internet safety, often in partnership with other agencies. Many companies, for instance, play an active role in both national and European level activities related to Safer Internet Day. However, in addition to high-profile events, many companies have developed ongoing relationships with organisations and groups in their local markets that act as a crucial means of engaging more directly with local child welfare NGOs and education providers.

A range of examples was presented by companies to illustrate the potential for this type of engagement with the wider community.

- KPN has a longstanding partnership with the Dutch Mijn Kind Online foundation and has produced over the years a wide variety of materials and resources for education. It is also a co-founder and partner in the Digibewust programme[13], a partnership between government, business and civil society encouraging safe and responsible use of ICTs.
- In 2013, Telecom Italia launched a largescale initiative, Anche Io Ho Qualcosa Da Dire (I've Something To Say, Too), which through a series of rolling workshops throughout the country brought technical experts into schools to promote safe and responsible online use. The programme has been rolled out to a number of Italian cities in the form of a weeklong tour in each location.
- Portugal Telecom's Comunicar em Segurança (Communicating Safely)[14] is a corporate volunteer programme to promote safe and responsible use of ICTs. The programme, begun in 2008, takes place in a classroom environment for the early years of secondary level. It gives the Portugal Telecom Foundation an opportunity to remain close to young people. Other initiatives undertaken include theatre role-playing about cyber bullying in schools and in municipal theatres, and Minuto Seguro (Safe Minute), a set of around 50 one-minute videos with tips on safety for educators and young people.
- In Slovakia, Slovak Telekom, part of the Deutsche Telekom Group, runs the kids portal, Rexik, which provides safe, positive content for kids. It has also partnered an educational project aimed at younger children and their parents called Sheeplive[15]. This is an award-winning resource that uses popular cartoon formats, games and fun content to communicate messages about internet safety. It is now available in 22 different languages.
- Also in Slovakia, Orange Slovakia has a major, long-term education project for schools aimed at improving children's understanding of safer internet use. This involves presentations to both primary and senior schools (reaching around 3500 pupils every year), under the guidance of 20 qualified psychologists. Orange Slovakia has also worked with the Children of Slovakia Foundation to develop a training programme and lesson handbook for teachers on media education. The aim is to implement and broaden the educational curriculum for primary and/or secondary schools on media education, protecting children from inappropriate content on the internet and ensuring safer and meaningful use of modern information technologies.

Another activity to raise awareness of internet safety is direct company support for research, which establishes another valuable partnership between industry and the wider stakeholder community.

An example supplied by Bwin.Party describes how in collaboration with the Division on Addiction (DOA) at Harvard Medical School, the company has, since 2005, supported research on gaming in online sports betting, casino, poker and other games. This has enabled the DOA to gain access to anonymised data for research purposes and to conduct ongoing research on actual gaming behaviour. This has been of benefit to both sides, providing the company with research support for its responsible gaming promotion while giving researchers access to otherwise difficult-to-reach audiences.

[13] https://www.digivaardigdigiveilig.nl/

[14] http://comunicaremseguranca.sapo.pt/

[15] http://www.sheeplive.eu/

Summary

Education and awareness raising is something that companies have wide experience of. Accordingly, they offer a comprehensive set of resources and materials particular to their own product range.

- Resources for education and awareness-raising primarily take the form of online materials accompanying their products and services which support safe and responsible use. Many companies have also developed extensive printed materials that have both promotional and educational value.
- The main target group for education and awareness-raising is parents, followed by teachers and teenagers. Parents are the primary focus for many companies. It is parents that companies are most likely to have a contract with (e.g. in the case of connectivity providers) and it is in this context that an extensive range of user education and support has been developed.
- Companies have entered into a series of partnerships with other groups, agencies and industry consortia for the development and delivery of training, education and awareness-raising. Such partnerships appear to be an excellent way of building critical mass and scale, providing a framework for engagement with the wider community and offering a cohesive message about online safety and responsible ICT use.
- Some good examples exist of companies supporting research through sharing of data and expertise.

Overview of selected features: Principle 6

	Provide education and awareness				Topics						NGO partnerships
Company	Under 13s	Teens	Parents	Teachers	Online safe behaviour	Privacy	Cyber-bullying	Down-loading/ copyright	Safe mobile use	Contact with strangers	
Bwin.Party											🟩
Deutsche Telekom			🟩	🟩	🟩		🟩		🟩		🟩
Facebook	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩			🟩
Google		🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
KPN			🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩
LG Electronics			🟩						🟩		
Nokia		🟩		🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Orange		🟩		🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Portugal Telecom	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
TDC	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩	🟩	🟩
Telecom Italia	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Telefónica	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Telenor	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
TeliaSonera	🟩	🟩	🟩		🟩	🟩	🟩		🟩	🟩	🟩
Unibet											
Vodafone	🟩		🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩

Note: categories refer to implementation at the group level and may not be available in all markets. See individual company reports for details.

Conclusion

The final section of this report presents conclusions and recommendations arising from the assessment of the ICT Principles, and reflects on the contribution they make to the topic of child online safety.

The ICT Principles were developed as an initiative by members of the internet and communications industry, drawing on companies' experience of operating in markets right across Europe and of various self-regulatory schemes to combat online child abuse. They take account of feedback from governmental and third-sector stakeholders. They were intended to define at a conceptual level the main requirements for safety in the online world.

The argument for self-regulation in the technology sector has long been that internet companies are best placed to identify emerging trends and challenges and to apply the safeguards needed to ensure that industry continues to develop and innovate in a free and highly competitive environment while fulfilling public policy objectives such as internet safety. Anticipating the rapidly converging technologies of information, communication and entertainment, the ICT Coalition has sought to identify the basic requirements and central areas of focus in which member companies can contribute to and mark progress on attaining better overall safety standards.

To this end, the ICT Coalition has been an undoubted success. It has fostered close cooperation between companies that, in commercial terms, are competitors in the same market arena. It has set out broad areas of agreement and common action on themes of safety and online protection that have been the subject of policy debate for many years. One of the main achievements in this regard has been the consensus on the problems to be addressed and the strategies required to address them. Many member companies in the ICT Coalition have extensive experience in online child protection, stretching back to the early 2000s. Bringing this experience to bear on an ever-diversifying market, with increasingly complex interrelationships between the different players in the internet ecosystem, is an important step in consolidating progress, agreeing standards and setting out a roadmap for future development.

Achievements

Successes achieved to date are illustrated in a number of ways as detailed in this report. First, it is clear that companies have followed through on commitments made to implement measures to support themes under the ICT Principles:

- Solid progress has been made in ensuring that online content that may be unsuitable for children or young people – where available on members' services – is clearly flagged, and its access restricted and increasingly accompanied by appropriate labelling guidelines.
- Parental control solutions are well established as a core element of most member companies' provision with well-resourced information and guidance about their use and the role they can play in managing internet access, particularly by younger children.
- Reporting tools, similarly, have become essential elements wherever content is uploaded, posted or shared. Companies have established reporting tools at the core of their systems, as well as robust internal procedures to handle reports of misuse and abuse or violations of terms of service.
- Companies have demonstrated a solid industry consensus on tackling child online abuse. Well-established, rigorous procedures are in place, and there is clear evidence of strong, effective relationships with hotlines and law enforcement.
- ICT Coalition members have given serious attention to implementing industry-standard approaches to privacy protection. Content-sharing and social media platforms have incorporated a wide range of flexible and customisable privacy settings that can be adapted to suit individual user needs.
- Finally, ICT Coalition members have contributed extensively to educational and awareness raising support. Across each of the themes of the ICT Principles, it is clear that

companies have supported individual initiatives with information and resource material across their platforms. There are also some very strong examples of collaboration with external partners, demonstrating the potential to work collectively on raising awareness and developing skills in the area of online safety.

Areas for development

Signatories of the ICT Principles have made a significant effort to implement the ICT Principles comprehensively, as detailed in the targets announced by each company and as illustrated in the review of each principle.

Inevitably, some of these targets were ambitious and have not all been achieved by each member within the first year. The individual review reports published by each company on the ICT Coalition website provide an overview of the implementation status of specific measures.

Areas where further development is needed have also been identified throughout this report and include attention to the following:

- The mobile environment – with fast-evolving applications and devices, and increasing adoption by children and young people – presents a new area of challenge for online safety. Internet safety guidance does not always translate evenly children and young people's use of mobile devices. It is not feasible, for instance, for parents to monitor and supervise young people's mobile access in the same way as for home-based PCs. There is a need, therefore, to ensure that implementation of safety features for mobile products and services are designed and tested to be as accessible and effective as their 'desktop' equivalents.
- Parental controls in the mobile environment, for example, remain an area that require further development and testing. Some companies have begun to introduce their own or third-party solutions. However, full implementation has not yet been achieved. More research is also needed to assess the effectiveness of such controls in the mobile environment as a tool for fostering safety.
- Content classification, which is best established in the gaming sector, is somewhat more unevenly available in the content for mobile devices. While many individual ICT Coalition members have introduced or applied their own classification schemes, greater consistency on approaches is needed if such classification schemes are to helpful as aids to safety for end users.
- While content controls and classification schemes are better established for certain categories of online content (e.g. professionally produced, own or third party content), they are much less developed for the whole area of user-generated content. This is a subject the industry as a whole has begun to address. Good practice is demonstrated by some of the the major platform providers in the ICT Coalition. However, an overall solution to ensure better information, classification and labelling is an area in need of improvement by the ICT Coalition and industry as a whole.
- Reporting tools and mechanisms are widely deployed across ICT Coalition members' products and services. What was less clear from the assessment was the effectiveness of their operation. Introducing greater transparency into how the reporting systems operate, levels of reporting and categories of reports would be an important step forward.
- Supporting privacy in all products and services is another issue that will require ongoing attention and development. The GSMA's Mobile Privacy initiative, promoting an industry-wide approach to privacy for mobile devices and apps design, is an important contribution. The interdependent nature of the internet eco-system means, however, that ongoing cooperation across industry is needed to build consensus and better implementation of privacy standards .
- While extensive education and awareness-raising resources are in evidence, more research into their effectiveness and take-up by parents and young people is needed. Previous research has shown that parents are much more likely to get information about internet safety from friends and other family sources and from traditional media (which may be biased) rather than from providers of actual services (Dueräger & Livingstone, 2012). Additionally, it would be helpful if the well-resourced, predominantly English-language (US or UK-based) materials for education – those, for instance, supported by Facebook and Google – were also available in other languages. To be truly effective, such resources should be developed with local partnerships in mind and in the languages of the different markets in which the products and services are offered.

Recommendations

Nothwithstanding the need for further development, the first report of the implementation of the ICT Principles presents a very positive picture. The initiative of the ICT Coalition in promoting a sector-wide response to targeted areas of e-safety implementation is a very valuable contribution that should be sustained and developed further into the future. It is important to build on the progress made to date and the cooperation that has developed between companies and the wider circle of stakeholders active in this field. The expansion of the ICT Coalition to 22 members representing different dimensions of the internet industry is a very positive sign and an opportunity to further build consensus and concerted action on the themes addressed by the ICT Principles.

In recognition of the important contribution the ICT Coalition makes to advancing an industry-wide consensus on child online safety, the following recommendations are made in support of that effort:

- The ICT Principles have been formulated in a general way so as to be flexible and to be capable of adaptation as the environment evolves. However, this generality means that they can be interpreted quite differently. It would be helpful, therefore, if, in addition to committing to the Principles themselves, companies developed an agreed framework for action based on specific, measurable and objective outcomes. This could take the form of a rolling action plan to which members subscribe, and identify areas of particular relevance to their services.
- Developing this action plan places a requirement on ICT Coalition members to translate the Principles into actionable, time-bound commitments, as illustrated, for instance, by the approach adopted by the Deutsche Telekom Group for the purposes of this implementation.
- For manufacturers, this could mean adopting measures to define standards for content and application design specifications. For network operators, it could mean prescribing measures within existing frameworks of regulation that can be most readily implemented to prioritise online safety. For content and service providers, it could entail defining conditions of access to content especially for the mobile environment to include appropriate labelling and reporting channels.
- An important achievement of the ICT Coalition has been the creation of a forum for knowledge exchange and sharing of experience between industry partners on internet safety developments. Sustaining this activity across the whole eco-system for connected devices should be a priority for the Coalition, expanding membership where possible and incorporating emerging platforms and areas of development including gaming platforms, device manufacturers, and apps and content developers. The opportunities for promoting the message of online safety at an individual company and collective level are substantial and will have wider benefits in instilling trust and confidence in the products and services used by children and young people.
- A further achievement of the ICT Coalition has been to collate a substantial amount of data relating to individual company implementation relating to the central principles of child online safety. The current report has synthesised and assessed these findings to document the current state of the art from a company perspective. Sharing of information regarding the nature of reports received by companies, the take-up of parental controls and other safety features, would be an important step forward. Without compromising data protection or information regarding internal company processes and procedures, the ICT Coalition should foster further partnerships with researchers and other stakeholders to advance knowledge of new and emerging risks in the online environment.

References

Duerager, A., & Livingstone, S. (2012). How can parents support children's internet safety? Retrieved from http://eprints.lse.ac.uk/42872/

European Commission. (1996). Green Paper On The Protection Of Minors And Human Dignity In Audiovisual And Information Services COM(96) 483.

European Commission. (1999). A Multiannual Community Action Plan On Promoting Safer Use Of The Internet By Combatting Illegal And Harmful Content On Global Networks. 4-year Work Programme 1999-2002.

European Commission. (2013). Green Paper COM(2013) 231 final. Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values.

Livingstone, S., & Haddon, L. (2009). *EU Kids Online: Final report. EC Safer Internet Plus Programme Deliverable* D6.5. LSE, London: EU Kids Online.

Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2013). *In their own words: What bothers children online?* LSE, London:*EU Kids Online.*

Miyazaki, A. D., Stanaland, A. J. S., & Lwin, M. O. (2009). Self-Regulatory Safeguards And The Online Privacy Of Preteen Children. *Journal of Advertising,* 38, 79–91.

Shin, W., Huh, J., & Faber, R. J. (2012). Tweens' Online Privacy Risks and the Role of Parental Mediation. *Journal of Broadcasting & Electronic Media,* 56, 632–649.

Smith, P. K., & Steffgen, G. (2013). *Cyberbullying Through the New Media: Findings from an International Network.* Psychology Press.

Appendix A
Methodology

Assessment Goals

The goals of the assessment were identified as follows:

1. To carry out an independent assessment of the company self-declaration reports submitted by each Coalition member on their company's implementation of the ICT Principles
2. To facilitate a transparent process of third party stakeholder and NGO input into the evaluation of company implementation of online child safety features
3. To provide feedback to ICT Coalition members on implementation levels, examples of good practice and areas for improvement in designing effective digital safety features for children and young people
4. To highlight areas of emerging challenge for online
safety for children through both technological and user trend analysis
5. To disseminate through a public report effectiveness of implementation under the ICT Principles.

Assessment Plan

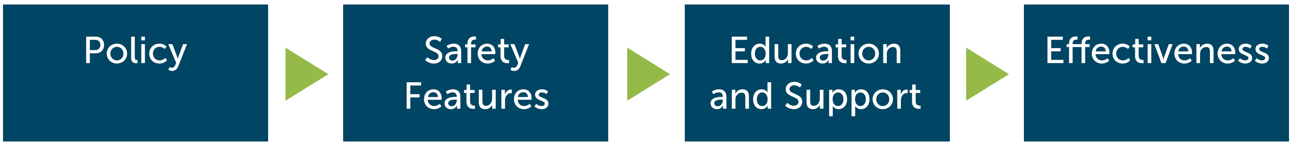
The ICT Coalition comprises company members from Accordingly, the ICT Principles have been set at a high level to enable the widest participation and to ensure that child online safety is incorporated in all dimensions of the technological environment.

Given the diverse mix of companies within the ICT Coalition, encompassing online service provision, content provision, network operation and manufacturing, the assessment plan, therefore, avoided direct comparison or benchmarking between companies and instead focused on:

a. The individual company level taking a holistic view of how implementation and achievements under the ICT Principles contribute to online child safety.
b. The sectoral level whereby distinct industry sectors - hardware manufacturers, network providers and service/content providers - demonstate levels of safety implementation.

Following the logic of the commitments outlined in the ICT Principles, the assessment of each company's implementation will focus on the following key aspects:

Figure 1: Key Aspects of the Assessment



The assessment process involved the following four main steps:

1. **Document review:** Collation of self-statements and related policy statements from individual Coalition members. Development of an agreed template for reporting.

2. **Company reports:** assessing self-statements and company submissions against the Principles.

3. **Stakeholder Feedback:** Consultation with appropriate stakeholders, inviting comments from third parties on the submitted reports. Facilitation of dispute resolution, where applicable, between companies and stakeholders, with regard to implementation of Principles prior to finalisation and publication of the assessment report.

4. **Testing and evaluation:** assessing implementation through observation and evidence.

The objective of the process was to achieve an independent evaluation of each company's achievements in implementing the ICT Principles for safer use of connected devices by children and young people.

The evaluation and testing took into account any observations of third parties and, where any significant discrepancies arose, mediation and outcomes, it was agreed, would be incorporated into the final report. As it happens, no such disagreements arose during the implementation period.

In addition to benchmarking and assessment at the individual level, the ICT Principles lend themselves also to a wider assessment of industry progress in attaining greater levels of online safety provision. Mapped against technological and user trends in a fast moving environment, the final report also seeks to highlight milestones and achievements of the sector in digital safety, taking into account international policy deliberations as well as emerging risks identified in global research on the landscape for youth ICT engagement.

Appendix B
ICT Coalition Members

The ICT Coalition is made up of 22 companies from across the information and communications technology (ICT) sector, including:

- AVG
- BBC
- Bwin.party
- Disney Club Penguin
- Deutsche Telekom
- Facebook
- Google
- KPN
- LG Electronics
- Nasza Klasa SP Zoo
- Orange
- Portugal Telecom
- Skyrock
- TDC
- Telecom Italia
- Teléfonica
- Telekom Austria Group
- Telenor
- TeliaSonera
- Unbet
- Vodafone