

# Child Safety Online

---

**A Practical Guide for Providers of  
Social Media and Interactive Services**

The UK Council for Child Internet Safety (UKCCIS) would like to thank our Social Media Working Group members below for their expert contributions to this guide.

The guide reflects their online child safety approaches in 2015, for you to consider and use as appropriate.

UKCCIS is a group of more than 200 organisations from across government, industry, law, academia and charity sectors, working in partnership to help keep children safe online.

## UKCCIS Social Media Working Group members

**Chair:** Ofcom - Claudio Pollack, Group Director, Content, Consumer and External Affairs

**Project Team:** Ofcom - Tony Close, Director of Content Standards, Licensing and Enforcement; Sarah Andrew, Head of On demand and Online Standards; Silvia Fukuoka, Associate, On demand and Online Standards, Ofcom

**Application Developers Alliance** – Martin Wrigley, General Manager; Claudia Trivilino, European Policy Manager

**Ask.fm** - Annie Mullins, OBE, Director of Trust and Safety

**BBC** – Matthew Eltringham, Policy

**BBFC** - Graham Hill, Policy and Public Affairs Officer

**CEOP** - Kate Sinnot and Annabel Wilson (Partnerships)

**Childnet International** – Will Gardner, CEO

**Children's Charities' Coalition on Internet Safety (CHIS)** – John Carr, OBE, Secretary

**Consultant** – Julian Coles

**Disney Club Penguin** – Ellen M. Blackler, Vice President Global Public Policy

**Facebook** – Rishi Saha, Head of Public Policy, UK

**FOSI** – Dave Miles, Director, Europe

**Google** – Katie O'Donovan, Public Policy and Government Affairs Manager

**IWF** – Kristof Claesen, IWF, Press and Public Affairs Manager

**London School of Economics** – Sonia Livingstone, OBE, Professor of Social Psychology

**Microsoft** - Becky Foreman, Head of UK Government Affairs

**NSPCC** – Julia Fossi, Senior Analyst, Online Safety

**Ofcom** – Alison Preston, Head of Media Literacy Research

**Parent Zone** – Vicki Schotbolt, CEO

**SuperAwesome** – Rebecca Newton, Head of Trust and Community

**Trust Elevate** – Rachel O'Connell, Founder and CEO

**Twitter** – Nick Pickles, Public Policy Manager

**UKCCIS Secretariat** – Anna Payne (Head of Child Internet Safety); Ellie Mond (Department of Culture, Media and Sports); and Anna Strudwick (Home Office, Safeguarding Unit)

**UKIE** – Andy Tomlinson, Public Affairs and Policy Officer

**South West Grid for Learning** – Laura Higgins, Online Safety Operations Manager

### With special thanks to the following for their commitment and support in producing this guide:

Andrea Parola (ICT Coalition), Dr. Angharad Rudkin, Chartered Clinical Psychologist (University of Southampton), Duncan Heppel (Kidslox), Jonathan Baggley (CEOP), Dr. Richard Graham (Consultant Child & Adolescent Psychiatrist, The Tavistock and Portman NHS Foundation Trust Tavistock Centre), Andrew Bruce (Advertising Standards Authority), Garreth Cameron (Information Commissioner's Office), Guy Levin (COADEC), Mind Candy, Nina Sivec (Outfit 7) and Seun Oshinaike (Silent Secret).

The research in this guide's [Annex](#) has been collated by the UKCCIS Evidence Group, a body which includes representatives from academia, government, NGOs and industry. You can find summaries of relevant research in the area of children's online safety on its website at <http://www.saferinternet.org.uk/research>.

## The ICT Coalition Principles

This guide uses the safety framework of the [ICT Coalition for Children Online](#), a European industry initiative to make its platforms safer for users. Members self-declare how they meet the guiding principles, and are subject to a review by an external auditor.

This framework includes six principles: Content, Parental Controls, Dealing with Abuse/Misuse, Child Abuse or Illegal Contact, Privacy and Control, and Education and Awareness. This guide builds on these principles, illustrating them with advice and industry examples.

The Annex includes more information, including contact details of how to become a member of the ICT Coalition if your business is based in Europe and meets its criteria.

### The Purpose of This Guide

A childhood with the internet is still a relatively new experience. Few households were online even 20 years ago.

The immediacy and reach of social media has opened up all kinds of positive opportunities for children as they grow, but also the possibility of considerable harm. Bullying, child sexual abuse, sexual grooming, trafficking and other illegalities can, and do, thrive if left unchecked.

Of course, it isn't the medium itself that presents possible danger, but the way it is used. This practical guide has therefore been designed to help you ingrain online child safety into your web or mobile business.

It's for you if you provide an online/mobile social media or interactive service (e.g. a social network, messaging, Q&A site, interactive game, cloud service or ephemeral messaging service) and your users are under 18 years old. You'll also find the guide useful if your primary audience is not the under-18s, but you still attract them.

Please note the guide does not replace legal advice, which you may still need in order to meet compliance and other requirements.

# The Guide at a Glance

Here is a quick reference summary to the guide's six key safety principles. In [Section 2](#), we expand on each of them, with case study examples.

## 1. Managing Content on Your Service

- Decide what content is acceptable on your service, and how you'll make this clear to users.
- Be clear on minimum age limits, and discourage those who are too young.
- Consider different default protections for accounts that are opened by under 18s.
- Plan and regularly update how you'll manage inappropriate or illegal content posted on your site.
- Consider using available age verification and identity authentication solutions.
- Plan now for dealing with illegal content.
- For under-13s, consider a walled garden environment and pre-moderating content before users see it. Also become familiar with the UK rules to advertising to children.

## 2. Parental Controls

- Consider parental controls that are designed for your service.
- Be aware how different parental controls might interact with your website or app.

## 3. Dealing with Abuse/Misuse

- Explain to users the type of behaviour you do and don't allow on your service.
- Make it easy for users to report problem content to you.
- Create a triage system to deal with content reports.
- Work with experts to give users additional information and local support.
- For under-13s, talk in their language, and pre- and post-moderate their content.

## 4. Dealing with Child Sexual Abuse Content and Illegal Contact

- Give your users a standardised function for them to report child sexual abuse content and illegal sexual contact.
- Have a specialist team, who are themselves supported, to review these reports.
- Consider technology such as PhotoDNA and working with relevant bodies such as the Internet Watch Foundation (IWF) to help remove child sexual abuse content.
- Escalate reports of child sexual abuse content and illegal sexual contact to the appropriate channel for investigation.
- Tell users how they can report child sexual abuse content or illegal sexual contact directly to the relevant authorities and/or where to obtain further advice.

## **5. Privacy and Controls**

- Only collect the personal data you actually need for your service.
- Tell users what information you collect, why and how long you'll keep it.
- Give users reasonable choices about how to use their personal information and specific types of data, such as geolocation data.
- Offer privacy settings options, including privacy-by-default, to give control to your users.
- Involve parents/guardians if you collect personal data from under-18s.
- For under-13s, have stricter privacy measures to help them understand the implications of sharing information.

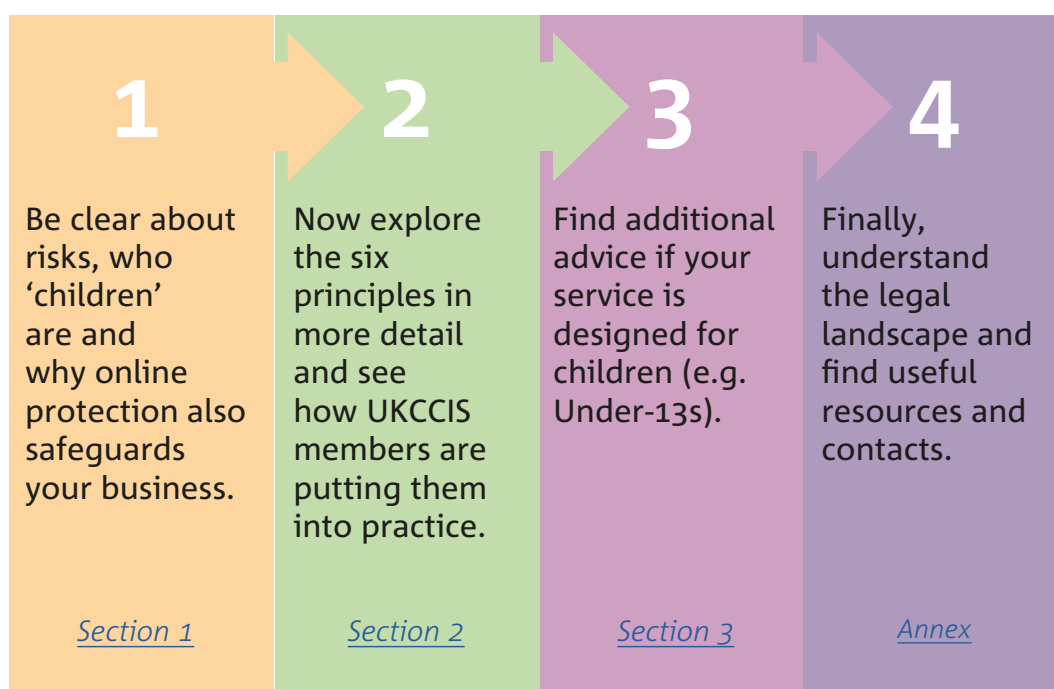
## **6. Education and Awareness**

- Educate users about safety as part of the experience on your platform.
- Work with parents, educators, users and their communities to raise awareness about online child safety.
- Work with experts to help develop your messages and to reach different communities.
- For under-13s, tailor the language and approach so they will take an interest.

<b>Section 1: About This Guide</b>	<b>6</b>
How to Use This Guide	6
How the Guide Can Help You	7
Who are “Children and Young People”?	7
Defining and Differentiating ‘Online Risks’	7
<b>Section 2: The Guide in Full</b>	<b>9</b>
<i>An expanded explanation of the six principles, with case examples from UKCCIS members.</i>	
1. Managing Content on Your Service	10
2. Parental Controls	14
3. Dealing with Abuse/Misuse	17
4. Child Sexual Abuse Content or Illegal Contact	23
5. Privacy and Controls	27
6. Education and Awareness	31
<b>Section 3: Under 13s - Additional Advice</b>	<b>35</b>
<i>Guidance on deeper safety and controls to protect the youngest users of your platform.</i>	
<b>Annex</b>	<b>44</b>
<i>Reference information, resources and contacts.</i>	
1. Legal Landscape. A summary of key UK legislation	45
2. Child Development Chart. How children and their attitude to risks evolve throughout childhood.	53
3. Evidence Section. Social media risks research	56
4. Examples of Tools Used by Social Media Service Providers	57
5. Contacts and Links	58

# Section 1: About This Guide

## How to Use This Guide



## How the Guide Can Help You

The way you design your service can have a real impact on children and young people. The type of safeguards shown in this guide lead to immediate positive benefits (e.g. limiting exposure to inappropriate content) and longer-term effects (such as helping users to understand how to share their information responsibly).

But online safety is also critical to your platform's future, and this guide will be particularly useful to:

- protect the health of your brand, and reassure sponsors, advertisers and investors who all need to consider their own reputational risks;
- implement the basics (and more) of safety policies and procedures before launching your service;
- overhaul or strengthen existing user safeguards;
- give confidence to both users and parents that you can manage safety risks; and
- implement even tighter safety provisions for users under 13 years old.

## Who are “Children and Young People”?

Our focus for this guide is to protect the under-18s.

However, children and young people have significantly different capabilities and expectations. We therefore give additional safety advice for children under the age of 13. ([Section 3](#))

Although this age has no specific legal bearing in the UK, it is the threshold used by many social media and interactive services. Since many are based in the United States, they follow the Children's Online Privacy and Protection Act of 1998 (COPPA), with its special safeguards on data collection for children under 13. (Please see the [Annex](#) for more information on COPPA.)

Clearly, reaching young audiences needs words, visuals and a tone of voice that's appropriate for their age. You will find examples across the guide.

## Defining and Differentiating ‘Online Risks’

Online risk<sup>1</sup> can be classified in three ways:

- **Content risk:** children receiving mass-distributed content. This may expose them to age-inappropriate material such as pornography, extreme violence, or content involving hate speech and radicalisation.
- **Conduct risk:** children participating in an interactive situation. This includes bullying, sexting, harassing, being aggressive or stalking; or promoting harmful behaviour such as self-harm, suicide, pro-anorexia, bulimia, illegal drug use or imitating dangerous behaviour. A child's own conduct online can also make them vulnerable - for example, by over-sharing their personal information or by harassing or bullying themselves<sup>2</sup>.
- **Contact risk:** children being victims of interactive situations. This includes being bullied, harassed or stalked; meeting strangers; threats to privacy, identity and reputation (for example, through embarrassing photos shared without permission, a house location being identified,

<sup>1</sup> For more information on the classification and definition of ‘online risks’, please see <http://eprints.lse.ac.uk/39410/>

<sup>2</sup> For more information on ‘self-harassment/bullying’ or ‘digital self-harm’, please see [http://vc.bridgew.edu/cgi/viewcontent.cgi?article=1004&context=marc\\_reports](http://vc.bridgew.edu/cgi/viewcontent.cgi?article=1004&context=marc_reports)



someone impersonating a user, users sharing information with strangers); and violence, threats and abuse directly aimed at individual users and/or groups of users.

- This guide also addresses risks associated with commerce such as online advertising and advertising to children (See Principle 1 and Section 4). For more information on the risks classification and other types of online risks, see the [Evidence Section](#) in the Annex.

### **Illegal contact, conduct and content**

Some online risks can not only lead to harm, but also result in illegal activity such as:

- sexual grooming and sexual exploitation;
- creation and distribution of child abuse images;
- online aspects of child trafficking;
- physical and mental abuse of children;
- selling and distributing illegal drugs; and
- revenge pornography, harassment and malicious communications.

Of course, many factors influence how potential online risks may or may not affect an individual child or young person. Their age, developmental stage and personal attitudes to risk all come into play. For further information, please see the Child Development Chart and Evidence Section in the [Annex](#).

# Section 2: The Guide in Full: The Six Principles

This section has good practice advice illustrated with examples.

<b>How many children are online?</b>	87% of children aged 5-15 go online via any type of device. (67% of 5-7s, 91% of 8-11s and 98% of 12-15s). <i>Ofcom, 2015</i>
<b>How important are their smartphones?</b>	One third (34%) of online 12-15s say that their mobile is their main device for sending or posting messages to other people. This compares to 4% saying their laptop/PC and 5% saying their tablet. <i>Ofcom, 2015</i>
<b>How important are their tablets?</b>	Given the ease of use of tablets, young children are using them independently at a younger age than other devices, with parents having little awareness of what they are doing. Gaming is particularly important to younger children, again largely on tablets <i>Livingstone, Marsh et al, 2014</i>
<b>What are they doing online?</b>	As we know, many are playing games and using social media. Half (48%) of online 9-16s say they visit a social networking profile daily, rising to 78% of girls aged 13-16. Over one quarter (27%) say they play games with other people online, rising to 50% of boys aged 13-16. <i>Livingstone, Haddon et al 2014</i>

# 1. Managing Content on Your Service

What kind of content is OK on your platform? And what isn't?

Every service needs to start with a clear definition of what is acceptable. You can then create a safer environment where users can share, while keeping age-inappropriate material away from children and young people.

Of course, content comes from many sources (from you, your users, your advertisers, third party plug-ins...) and in many forms (video, photos, music, games, live chat and messaging, votes and comments, Tweets, memes, gifs...). You need to know how you will manage content in all its complexity.

Remember also that content can leave a permanent record, even on time-limited platforms. For example, users may download material or create screenshots.


<p><b>How many children are seeing negative types of content online?</b></p>	<p>Just over one in ten (12%) of online 9-16s say they have seen sexual images online.</p> <p>The same proportion of online 11-16s (12%) said they'd seen websites where people talk about taking drugs, and 17% had seen sites where people discuss ways of physically hurting themselves.</p> <p>4% said they'd seen websites where people discuss ways of committing suicide, and the same proportion (4%) said they had received "sexting" messages</p> <p>While these figures may not appear headline-grabbing, they nonetheless represent sizeable numbers of children. In an average class size of 30 children, it means that:</p> <ul style="list-style-type: none"> <li>• approximately three children have seen online sexual images;</li> <li>• five children have encountered sites about physical harm,</li> <li>• and one child has received sexting messages</li> </ul> <p style="text-align: right;"><i>Livingstone, Haddon et al, 2014</i></p>
<p><b>What do parents think of social media sites?</b></p>	<p>In 2015 the NSPCC carried out a project in conjunction with Mumsnet to ask parents to view and rate the 60 most popular social media, games and apps that children use. It found that:</p> <ul style="list-style-type: none"> <li>• parents saw sexual content in 72% of the sites,</li> <li>• bullying in 52% of sites,</li> <li>• and violent/hatred content in 52% of sites.</li> </ul> <p style="text-align: right;"><i>NSPCC, 2015</i></p>
<p><b>What are parents using and doing?</b></p>	<p>Overall, nearly all parents say they are doing something – either using technical tools, talking regularly to their child, supervising them, or having specific rules in place.</p> <p style="text-align: right;"><i>Ofcom, 2015</i></p>

## Good Practice

### 1. Decide what's acceptable and what isn't.


- Plan your service so that your content, and your users', is suitable for your target audience. Enable a virtuous circle where good behaviour starts to encourage more of the same. See some examples below.
- Gauging what is suitable can be difficult. See the BBFC criteria on how they distinguish between under-18s and under-12s. See also Section 4 for more advice about under-13s and under-7s.
- If you have content that is not appropriate for under-18s, see point 7 below. Also consider the type of moderation (see [Section 3](#)) you might want to apply

#### Examples

 The [BBC's House Rules](#) for their message boards state that "Racist, sexist, homophobic, disablist, sexually explicit, abusive or otherwise objectionable material will be removed and if extreme will result in immediate and permanent restriction of your account."



For other examples of what services do and don't allow, see the [Twitter rules](#), Facebook's [Statement of Rights and Responsibilities](#), or YouTube's [Community Guidelines](#).

 The British Board of Film Classification (BBFC) has different frameworks for content accessed via mobile networks in the UK. Both are based on their Classification Guidelines for film and video, and define what's unsuitable for under-18s, and under-12s. Content they consider unsuitable for under-12s includes: detail of potentially dangerous behaviour including depiction of self-harm; discriminatory language or behaviour; sight of sexual activity unless discreet; sexualised nudity or posing; moderate or strong violence or language; and references to sexual violence. You can see their full criteria [here](#).

### 2. Regard advertising as another source of content on your service and know how it is regulated.

- Make sure you're up to date on the mandatory UK advertising rules and that you understand how they are applied online, as well as to email and direct marketing generally. For general information on advertising regulation, visit the Committee of Advertising Practice ([CAP](#)). They write and maintain the [UK Advertising Code](#), which is administered by the Advertising Standards Authority ([ASA](#)).

### 3. Tell users what to expect when they sign up, and explain what isn't allowed.

- Explain your rules in your Terms of Service, community standards or guidelines. Use suitable language for the ages you're talking to, and look for other places to share this information.
- Your rules should be clear, prominent and easily accessible – for example, via a link on the homepage, and in a safety or contact centre section, and where comments are posted.
- Use age ratings, descriptions and warnings to manage user expectations. Consider letting users self-rate content they upload.

- Take the chance to make frequent reminders of your rules. For example, when users sign up or see new content; or upload or share content with others, and so on.

#### Example



World of Warcraft will [warn or suspend](#) players who engage in obscene or vulgar language and/or reference illegal drugs. Severe violations include engaging in real-life threats; promoting racial, ethnic or national hatred; referring to extreme and/or violent sexual acts; insulting or negatively portraying someone based on their sexual orientation; or denigrating major religions or religious figures.

## 4. Be clear on minimum age limits, and discourage those who are too young.

- Web and mobile app services should consider using an age rating or content warning. If you are a gaming provider, you can obtain a classification from [PEGI](#).
- Most mainstream social media companies ask for a user's date of birth. Under-13s are usually denied the option to create an account, and any accounts found to belong to that age group are deleted. Services that are designed for under-13s have different approaches (see Additional Advice in [Section 3](#)).
- Take steps to deny access to children who lie about their age. For example:
  - » place a cookie so that a declined user can't attempt to reregister with different age details;
  - » use tools such as search algorithms to look for slang words typically used by children and young people, and to identify children under 13 who may have lied about their age at registration;
  - » offer free downloadable controls so parents can manage their children's use of the service (see [Parental Controls](#)); and
  - » stay informed about the development of a public standard for age verification by the British Standards Institute (e.g. <http://www.agecheckstandard.com>).

## 5. Consider default protections for accounts that are opened by under-18s.

This can protect the youngest users on your service from the moment they sign up. See also [Principle 5](#) for examples of this approach.

## 6. Plan and regularly update how you'll manage inappropriate or illegal content posted on your service.

- It's crucial to have trained staff to deal with reports of inappropriate content, and to have a clear process to take it down, block a user from posting or make a report to a relevant authority. Content reporting and take-down are covered in the next sections.
- Consider if your content management approach can include moderation, age verification or filtering systems, whether they're developed in-house or outsourced to commercial providers. The [Annex](#) includes examples of additional tools that can be used in the day-to-day operation of your service.
- Offer easy to use reporting mechanisms for inappropriate content (see [Principles 3](#) and [4](#)). These types of mechanisms are reactive moderation tools; see [Section 3](#)'s note on moderation.
- Offer automated warnings or blocks on certain kinds of content such as sexualised images;

restrict auto-playing of some videos on news feeds and timelines; and use a splash screen before graphic content.

- Use labelling and age-gating protections to shield younger users from content that is not suitable for them.

#### Examples



On Instagram, you cannot search hashtags that actively promote self-harm, such as “thinspiration,” “probulimia,” and “proanorexia”. Any hashtag associated with self-harm, whether attempting to promote it or not, shows a warning notice prior to the content becoming visible, as well as a link to external support websites.



YouTube, or indeed uploaders themselves, can age-restrict a reported video. This is true even if it does not breach the Community Guidelines, but is considered unsuitable for younger users.



On Facebook, content is reviewed by humans, and automated systems help detect and prevent hacking, phishing, spamming and fake accounts.



Microsoft will take action on behalf of victims when it is notified that content has been shared without permission (for example, ‘revenge porn’). They [remove](#) links to photos and videos from search results in Bing, and remove access to the content itself when shared on OneDrive or Xbox Live.



The BBFC, with Dutch regulator NICAM, is currently testing a [rating tool](#) to enable the public rating of user-generated content, and reporting of any inappropriate content.

## 7. Consider using available age verification and identity authentication solutions.

If you offer services aimed at adults (such as sexual content, dating, gambling or flirting sites), consider how to prevent access by users who are under 18.

- A credit card check, PIN numbers or proof of account ownership can help verify that users accessing adult content are indeed adults.
- Signing in with App Store Account that already encompasses an age gate and requires credit card data when registering.
- Signing in with a social media profile that already encompasses an age gate and doesn’t allow under-18s to create profiles when registering.

## 8. Plan now for dealing with illegal content.

Get legal advice on what content is illegal in the UK, and what you are required to do if you find it on your platform. See [Principle 4](#) for specific information on child sexual abuse and illegal sexual contact.

## 2. Parental Controls

Providing parental controls, ranging from software and browser tools to device-specific settings, has both a practical and perceived value.

As well as shielding children from unsuitable content, it is an outward signal to parents that your brand takes online safety seriously.

As well as your own controls, you might also consider how your platform interacts with third party controls offered by ISPs, device controls, and controls from other platforms.

Current parental solutions typically categorise material by age and content, and can restrict access to a service based on the information available on their site or app. They try to keep the overblocking, underblocking or mis-categorisation of websites to a minimum.

Its important to make sure parental controls are easy to use, and to offer guidance and resources to help families get the best from any parental controls you provide.


<b>What are parents using and doing?</b>	Overall, nearly all parents say they are doing something – either using technical tools, talking regularly to their child, supervising them, or having specific rules in place. 94% of parents of online 5-15s are doing at least one of these things, and one in three are doing most. That said, 12% of parents of online 12-15s do not do any of these things <i>Ofcom, 2015</i>
<b>Are they using technical tools?</b>	In terms of using technical tools specifically, over half (57%) of parents with home broadband use any type of technical tool, and over one third (36%) use content filters. Almost all parents who use them say they are useful, and three quarters (77%) say they block the right amount of content <i>Ofcom, 2015</i>
<b>Do parents know what their children are doing?</b>	Four in ten (39%) of online 7-16s said that their parents didn't know what they did online "always" or "most" of the time. <i>Wespiesser, 2015</i>


## Good Practice


### 1. Consider parental controls that are designed for your service.

Make sure they are easy to use to encourage take-up by parents.

#### Examples

 Google lets parents change their search engine settings on both the mobile and web versions to “Safe Search” mode, which can be locked on and protected by password. This can help block inappropriate or explicit images such as adult content from search results.

 BBC iPlayer has a Parental Lock facility that can be activated to block audio and video content accessed from a browser. It can be activated when the service is accessed from a computer, connected TV, games console, mobile or tablet. The BBC’s ‘G’ for Guidance labelling system is used to trigger parental PIN control systems.

 World of Warcraft offers a range of game specific parental controls to provide parents and guardians with easy-to-use tools to set up rules for play time, and to manage access. These may interact with your service and include time limits, voice chat, play time reports, real ID, and in-game transactions.


### 2. Be aware how different parental controls might interact with your website or app.


ISPs, mobile network operators, public Wi-Fi and application platforms offer bespoke parental controls solutions for their customers, and they may have an impact on your service.


#### Controls offered by application platforms

- How you age-rate or classify your app on application platforms informs the parental control tools that they offer to their customers:

#### Examples

 Apple requires developers to be responsible for assigning appropriate age ratings to their apps if they wish to offer them via the App Store. Inappropriate ratings may be changed/deleted by Apple. To see how this might affect you, please refer to [App Store Review Guidelines for Developers](#).

 The Google Play store requires games and apps to use IARC’s rating system to indicate the age-appropriateness of the content. You can find further information [here](#) on rating your app.

 Gaming platforms: consoles and handheld gaming devices offer age rating symbols and descriptor icons as part of their parental controls. These controls limit access to particular PEGI rated content, so having a [PEGI](#) rating on your game is essential.

#### Controls offered by ISPs

- To check if an ISP’s controls affect you, look at the content categories of ISP parental controls, including those of the four largest providers: [BT](#), [Sky Broadband Shield](#), [TalkTalk HomeSafe](#) and [Virgin Media](#).



- If their filters affect your site incorrectly, you can contact these four providers at [report@internetmatters.org](mailto:report@internetmatters.org).
- You can also check if your URL is restricted by an ISP in the UK at [www.blocked.org.uk](http://www.blocked.org.uk).

### **Controls offered by mobile network operators (MNOs)**

- MNOs in the UK have a default-on filter for material suitable only for adults, including sexually explicit material. Access to it requires the consent of an age-verified adult bill payer. EE, O2, Three and Vodafone operate controls by default when a new mobile phone is purchased in the UK, following the standards set by the BBFC's [Mobile Classification Framework](#).
- You can use the BBFC's [appeals and complaints](#) process, and seek their [advice](#), if you are concerned about access to your service being affected by parental controls.

### **Controls on public WiFi**

- You can check if your business is affected by the [Friendly Wi-Fi scheme](#). This is used by retailers and public areas where children are present. Filters automatically block their public Wi-Fi from showing any pornography and webpages that are known to the Internet Watch Foundation (IWF). (See also [Principle 4](#))

### **Additional controls**

Be aware of other controls that might have an impact on your service. These may include internet security software such as anti-virus, firewall and spam blockers on multi-device and multi-user parental controls solutions; controls related to online purchasing (including age checks); or limitations on hours of use. Parental controls may also be found in PCs, tablets, mobile phones, games consoles and internet-enabled hardware such as televisions, domestic appliances and wearables.

# 3. Dealing with Abuse/Misuse

‘Abuse/Misuse’ is inappropriate and illegal behaviour, including the social and psychological abuse of children and young people.

You should not ignore Abuse/Misuse. It has the power to cause distress and harm, exacerbating problems such as poor self-image, isolation and loneliness. It can lead to, among other things, self-harm and even suicide. Platforms have also noted the phenomenon of users who harass or bully themselves<sup>1</sup>.

## Abuse

This guide covers sexual abuse and contact specifically in [Principle 4](#), but the more general term of ‘Abuse’ covers a range of behaviours intended to be aggressive towards others. This may include:

- posting nasty and cruel comments to upset others;
- bullying (which includes excluding users intentionally from a group and also self-bullying);
- trolling;
- stealing personal information or content, and sharing it;
- impersonating someone to their detriment;
- online harassment or gossip; and
- physical or emotional abuse (such as hitting, choking, whipping, crushing, humiliating or verbally abusing a child).

Abusive behaviour can occur on any web or app service. It can be a subtle, yet still harmful, pattern of behaviour so it is important to consider its context; what might appear to be an innocent interaction can become trolling if the behaviour is predatory or persistent over a period of time.

---

<sup>1</sup> For more information on ‘self-harassment/bullying’ or ‘digital self-harm’, please see [http://vc.bridgew.edu/cqi/viewcontent.cgi?article=1004&context=marc\\_reports](http://vc.bridgew.edu/cqi/viewcontent.cgi?article=1004&context=marc_reports)

## Misuse

‘Misuse’ is about people deliberately using your service in the wrong way, often with the intention of abusing others. Examples of misuse include:

- intentionally using a service’s features to disrupt others;
- using anonymity to be cruel and unkind;
- creating fake profiles against the rules of the site; and
- hacking others’ accounts, abusive swearing, or creating multiple accounts for trolling.

Not all misuse of your service may be intended as abuse; make sure you give simple and clear explanations of your community standards to address this.

<p><b><i>What types of online contact are important to children?</i></b></p>	<p>Image management is vital to many children, and increases in importance as they grow older. Children continually update and check their profiles and the extent to which their photos have been liked.</p> <p>Particularly for girls, image is critical. For boys, appearing funny and laid-back is more important.</p> <p style="text-align: right;"><i>Ofcom/Sherbert, 2014</i></p>
<p><b><i>What types of contact are they having online?</i></b></p>	<p>One in four 12-15s who play online games do so against someone they’ve not met in person, as do one in ten 8-11s.</p> <p>Because many children use the same username across multiple games and social media (even if it is not their actual name), then it can be relatively easy to trace them.</p> <p style="text-align: right;"><i>Ofcom, 2015</i></p>
<p><b><i>Have they experienced negative contact online?</i></b></p>	<p>When asked directly:</p> <ul style="list-style-type: none"> <li>• 4% of all 12-15s and 1% of all 8-11s say they were bullied on social media in the last year.</li> <li>• Another survey, filled out online and with a sample taken from London schools, indicates higher levels of bullying – one in five of online 7-16s say they have been bullied online.</li> </ul> <p style="text-align: right;"><i>Wespiesser, 2015</i></p>

## Good Practice

### 1. Tell users at sign-up, and again through reminders, what content or behaviours constitute abuse and misuse of your service.

- Create rules or community standards prohibiting behaviour such as threats or harassment of others, hate speech, threats of violence, creating serial accounts to disrupt or abuse, or posting someone else's private information without permission (e.g. intimate photos or videos shared without the subject's consent).
- Tailor your rules to your users' age ranges and be in control of how your service should be used. If you offer content for adults, state this clearly and protect any users under 18 from coming across it.
- Equip your users to block, limit or manage the information they share (such as their profile details, location data, etc.) and how they interact with others (for example, disabling chat or other social functions such as tagging and being added as a friend).

#### Examples



See [Facebook](#), [Instagram](#), [YouTube](#), [Ask.fm](#) and [Twitter](#)'s rules for examples of what is and isn't acceptable behaviour.



The BBC has [House Rules](#) for their message boards. It considers abuse and disruption as using language likely to offend; harassing, threatening or causing distress or inconvenience; 'flaming' (posting something that's angry and mean-spirited); bumping or creating duplicate threads; or posting in such a way as to cause technical errors.

### 2. Prepare abuse reporting and take-down processes that your users and team understand.

- Have robust procedures in place for handling reports. Those about harassment and inappropriate content must be assessed fairly and promptly. If appropriate, offending content must be removed quickly.
- Child sexual abuse content and illegal sexual contact online should be dealt with immediately by people who have been appropriately trained, consistent with specific legal obligations (see [Principle 4](#)).
- Make sure you enforce your rules and be very clear about the reasons for your decisions.
- Remember that some users may be abusive unintentionally and just need a firm reminder about your rules on good behaviour. Others may also engage in self-bullying and self-harassment and will require a more considered response by your online child safety expert.

#### Examples



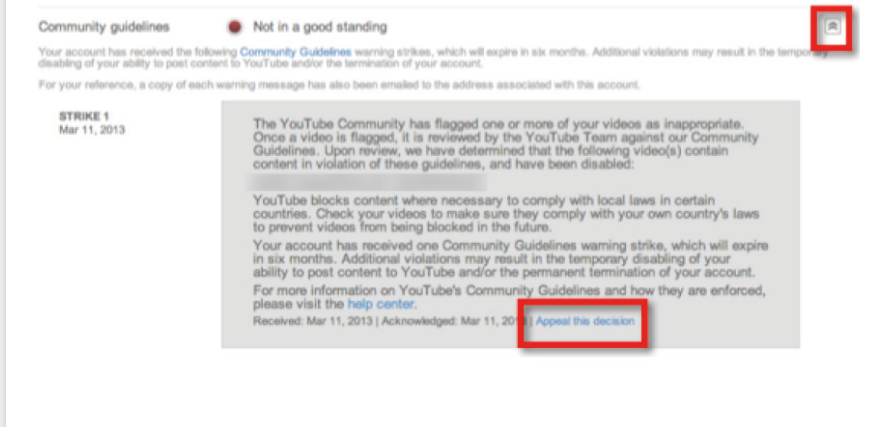
[World of Warcraft](#) warns and if necessary bans users who infringe their content policies. A sample message: "We suspend or ban accounts for violations of our in-game and forum policies. If you're seeing this message, check your email for details about the violation. If you think your account may have been hacked, secure your computer and account and then contact Customer Support." Players can follow an appeal process if they consider this unfair: "If you would like to appeal the action, review the appeal process before submitting a ticket."




Accounts are penalised for Community Guidelines violations, and serious or repeated violations can lead to an account being terminated. In that event, the user won't be allowed to create any new accounts.

## Appeal a strike

1. Visit your [Channel Settings](#)
2. Click the arrow next to the Community Guidelines section to show your strikes
3. Click the **Appeal this decision** link as shown below



 If a user has violated its rules, Twitter may take a range of actions; from a warning, to a temporary or permanent suspension of the account. They may also require users to take a specific action, such as to confirm that they have read and understood the Twitter rules, or to provide a phone number. In cases of impersonation, a user is asked to confirm their identity. If a user is reported for spam they will receive an on-screen notification confirming that a report has been received.


### 3. Make your abuse report system accessible and easy, and offer it regularly.


- Show a prominent icon next to all types of content for users to report any concerns. There are some broadly established industry signposts to highlight reporting mechanisms: Twitter and Instagram place three dots (⋮), while YouTube uses a flag (🚩).
- A general email address or online form can also complement reporting mechanisms.
- Ask users the reason for the complaint, the location of the content (e.g. the URL), type of content (e.g. photo, video, a post...), and any other relevant information. Some solutions can automatically capture key information and evidence, such as a screen grab, the online ID of the alleged abuser, and the date and time of the incident being reported.
- Confirm you've received the report and what you will now do with it. If possible give a time frame (e.g. in hours or days) of how long your enquiries will take. When complete, say how you've resolved the issue.
- Get the complainant's email in case you need further information.
- Act immediately if there is a threat to life or immediate risk to a user.


**If a child is in immediate danger, please dial 999 and ask to speak to Police**


- Report any illegal activity or suspicion to the police.
- Where appropriate, you can refer young users to Childline (0800 11 11), a free counselling service for under-19s, and inform adults that they can make a report anonymously about concerns for a child on the NSPCC Helpline (0808 800 5000).


## Examples

 The behaviour of the alleged abuser is assessed against the Community Standards, and the user is notified that Facebook has received a report. If in breach of the ToS or Community Standards, the offensive material and other content could be removed from their account. Complainants can access their 'Support Dashboard' to track how their report is being dealt with. Persistent abusive content or behaviour may result in a user being denied certain Facebook features (such as photo uploads), or losing their account altogether.

 Twitter users can report a contentious Tweet by selecting the three small dots in the bottom right corner. They can also control their experience by, for example, blocking or muting the user who posted the Tweet. They can also do this online through the Twitter Help Center.

 Has small flags beside every post and user profile. Users are also able to report posts, profiles or behaviours through the 'Contact us' feature on the site. Whether you're a logged-in user or a casual visitor you can report abuse, and threatening or unacceptable posts. Reporters receive an on-screen confirmation when their report is submitted.


 On YouTube users can click on the flagging feature under each video to select the type of guideline violation that they would like reviewed; this includes sexual content, spam or abuse, or infringement of rights. There is also a more detailed reporting tool (including abusive content and other classifications), a privacy complaint process and legal web forms.

 [Runescape](#) lets players communicate through a chat system. They choose who they will and won't interact with, without having to give out any personal details. They can also report any other players who are behaving in an inappropriate manner. There is no voice chat option in the game.


## 4. Have a clear reporting & escalation process that can respond to different types, and urgencies, of report.

- Have a well-understood internal reporting process with clear lines of responsibility. For example, a triage system can prioritise reports (both internally and to third parties such as law enforcement), by issue and urgency. Reports of cyberbullying, trolling or threats to life clearly require greater care and priority action. Alert law enforcement immediately about child sexual abuse or where a child is at risk of immediate harm. For example, see [Principle 4](#) to contact CEOP and the IWF.
- Follow your standards consistently. Give your staff an internal handbook explaining your safety processes, to refer to and use.
- Are your people equipped to handle this aspect of your operations? Are there enough of them and are they trained to understand and follow your procedures? How are you supporting them to cope with the content they are dealing with?
- You may need a policy and safety team to deal with these issues expediently and be compliant with the law. Seek legal advice on key areas that can have significant impact, such as data protection, privacy and defamation, and know what to do if you encounter illegal content and conduct on your service.
- Keep reporting mechanisms under review. Be ready to update them so you can respond to new trends and changing circumstances.

### Example - Getting a process in place

 Facebook: Community Operations teams are based in several locations across the world. They will see most reports within a few days, but strive to address the most urgent reports in a matter of hours. The most critical ones are actioned quickest, such as when there's the clear possibility of actual harm. Reports are mainly reviewed by a team of people, and they also use smart technology to take action against potential phishing links, scammers, phishers or fake accounts.


### Example - Training Staff

 Ask.fm has guidelines for all moderation staff on how to moderate specific types of content, such as image, text and spam. Training is designed with the input of safety experts and the staff themselves, to capture emerging new trends on the platform, and in the digital space in general.

## 5. Work with experts to give users additional information and local support.


- Consider if there are particularly vulnerable groups who may need extra support, such as children and young people with attachment, developmental or physical disorders.
- If you find users who need guidance on risks associated with Abuse/Misuse, consider referring them to helpful online resources. See the [Annex](#) for suggestions.
- As well as giving general information about staying safe on their platform, companies often work with local experts to provide specialist resources. For more, see our links to organisations in the [Annex](#).



### Examples


 Facebook has an [anti-bullying](#) hub and suicide prevention section in its [Help Centre](#).


Facebook has resources for people who may be at risk for a variety of reasons; for example, military personnel and their families, members of LGBT communities, and people vulnerable to suicide or self-harm. Facebook is also testing a new way for a potentially suicidal user to be directed to talk to someone, and/or to get appropriate support.

Facebook also hosts an annual Compassion Research Day, collaborating with safety experts to feed into product development and to understand risks.

 Ask.fm's Safety Center includes information and resources on specific risks such as bullying, self-harm and suicide. It also includes resources for law enforcement created by partners including iSafe, NetSmartz.org, and StopBullying.gov, and the results of work with others such as NCMEC, SpunOut and The Trevor Project site.

  Facebook and Ask.fm have set up Safety Advisory Boards, with online safety experts to consult on developing policies in this area.

 Instagram has a [Help Centre](#) and [blogs](#) about new safety features. They also collaborate with the Samaritans and include their details in their Help Centre. If a user has concerns about a friend or family member and reports a piece of content, they will be given a local number and website address.

 YouTube has a flagging system to report potential violations of its Community Guidelines. To make the process more efficient and effective, they created the Trusted Flagger Programme, giving members access to more advanced flagging tools as well as periodic feedback.

YouTube also has an enforcement team that reviews flagged videos 24/7. Each day they review more than 100,000 reported videos, and in 2014 removed 14 million videos that violated the Community Guidelines.

# 4. Child Sexual Abuse Content or Illegal Contact

It is important first to be clear on what the terms ‘child sexual abuse content’ and ‘illegal contact’ actually mean.

- ‘Child sexual abuse content’, refers to imagery or videos (or pseudo-images) that depict the sexual abuse of one or more children, and which is shared or distributed via an online platform. It is a criminal offence to take, permit to be taken, make, possess, show, distribute or advertise such images.

Child sexual abuse content is illegal and, therefore, it is illegal for you to host such content on your platform.

- ‘Illegal Contact’ refers to ‘illegal sexual contact’. It concerns the online sexual exploitation of children, where an offender will engage with a child via an online platform for purposes such as: making arrangements to meet in person for illegal contact; inciting the child to produce indecent images of themselves and send them to the offender; engaging in sexual activity and inappropriate chat; or blackmail/extortion of the victim by the offender, as a result of indecent images being shared.

To a child sex offender, your platform represents an opportunity to gain virtual access to children, to sexually exploit them and/or to share child sexual abuse content with others. You therefore have a vital role to play in protecting your users.

To do this you must have the dedicated resources to detect and prevent child sexual abuse content and child sexual exploitation.

Work alongside law enforcement partners and others to prevent these offences occurring on your platform, and report:

- suspected child sexual abuse content to the IWF (Internet Watch Foundation)
- suspected illegal sexual contact online to NCA-CEOP (National Crime Agency – Child Exploitation and Online Protection Command).

This will help ensure that abuse content is removed quickly, victims are protected and offenders are identified.



## Good Practice

Take these steps to identify and deal with child sexual abuse content and illegal sexual contact on your platform.

### 1. Give your users a standardised function for them to report child sexual abuse content and illegal sexual contact.

- Encourage user reporting by making sure there's a visible link to your reporting page throughout your platform. Consider including designated categories for child sexual abuse content and illegal sexual contact. Also consider linking directly to CEOP and the IWF so that users can make direct reports:
  - » CEOP: [www.ceop.police.uk/safety-centre](http://www.ceop.police.uk/safety-centre)
  - » IWF: [www.iwf.org.uk](http://www.iwf.org.uk)
- Confirm to users that you have received their report and provide a brief status update. If the report has not, or will not, be actioned, explain why. If additional information is required from the reporter, contact them directly.

### 2. Have a specialist team, who are themselves supported, to review these reports.

- Set up and train a team of staff to review user reports and give them regular training, and guidance material, to build on their expertise.
- Your staff may be exposed to distressing content - you have a duty of care for their welfare. Establish a comprehensive internal policy that includes regular one-on-one welfare reviews, desensitisation training, regular psychological assessments and access to 24/7 support services. Review this policy regularly to ensure it continues to be fit for purpose.
- Establish a process for receiving and assisting with law enforcement requests, such as user data, in accordance with existing laws and data protection rules. (See [Annex.](#))
- Enhance your capability by working with other industry stakeholders, and designated child protection bodies such as the IWF, to gain access to specialist tools and services. For example, IWF's Hash List and Keyword List.
- Consider using available technology to help detect child sexual abuse content more efficiently on your platform. For example, PhotoDNA technology, a Microsoft service that helps identify and remove known child sexual abuse images (Visit [www.microsoft.com/photodna](http://www.microsoft.com/photodna))

### 3. Escalate reports of child sexual abuse content and illegal sexual contact to the appropriate channel for investigation.

- Prioritise **all** actionable reports of child sexual abuse content & illegal sexual contact online (i.e. where an offence has been committed). If there are instances when you suspect that an activity could lead to illegal sexual contact, this should also be prioritised.
- Any report which indicates there is an immediate or high risk to a child, or children, should be identified and escalated to the police immediately
- If you operate such a triage system to action reports, based on indicators of risk and case-by-case assessments, this should be formalised in guidelines circulated to all your staff. These guidelines should also consider the protocols to be adopted when your staff refer a report directly to '999'.

- For more information on the UK’s legal framework for communicating child sexual abuse content to the relevant authority, see the [Annex](#).

**If a child is in immediate danger, please dial 999 and ask to speak to Police**

Once any imminent danger has been reported to the police, any suspected child sexual abuse content or illegal sexual contact online should then be reported as follows:

## **Child Sexual Abuse Content**

(e.g. images, videos, live streaming)

Report this type of content to the **UK’s Internet Watch Foundation**:

- Go to [www.iwf.org.uk/report](http://www.iwf.org.uk/report) and complete the online form, quoting the URL of the abuse content .
- IWF’s trained analysts then assess the content against UK law and pass on confirmed abuse to the relevant law enforcement authorities. You may later be contacted to help with their investigation.
- After notifying law enforcement, the IWF will send you a ‘Notice and Takedown’ request to remove content hosted in the UK.
- If the content is hosted abroad, IWF will work with its international partners to remove the content at source, and you can remove the link to the content from your platform.
- Data is captured for statistical purposes, and new child sexual abuse images can help build the hash set (database) of known child sexual abuse content.

### **IWF Members**

- You can also become a member of the IWF to collaborate more closely and obtain additional advice.
- IWF members have a designated email address for making reports. Members’ reports are treated as a high priority.
- IWF members have additional services, such as the Hash List, Keyword List and URL List that help prevent, detect or remove child sexual abuse content faster and more effectively.
- Visit [www.iwf.org.uk/join-us](http://www.iwf.org.uk/join-us) for more information or contact [members@iwf.org.uk](mailto:members@iwf.org.uk).

### **Retention of Content**

- You can remove the abuse content from your servers once you receive the ‘Notice and Takedown’ request from IWF, if you haven’t already done so, in the knowledge that the correct procedures have been followed.

## Illegal Sexual Contact Online

(e.g. sexual chat and video streaming, incitement to share images, arrangements to meet)

Report this type of content to the **UK National Crime Agency's – Child Exploitation and Online Protection (CEOP) Command**:

- Visit [www.ceop.police.uk/Ceop-Report](http://www.ceop.police.uk/Ceop-Report) and register your company's details
- Complete and submit the brief and secure online reporting form. When complete, you will receive confirmation.
- Provide the following level of information where available/applicable:
  - » Is the report urgent?
  - » Contact details of the reporting person
  - » Copies of chat logs between the victim/s and suspect/s
  - » Name/address/telephone number of the victim/s and suspect/s
  - » Email address of the victim/s and suspect/s, including confirmation that this email address is verified
  - » IP address of the victim/s and suspect/s, including the capture time and date.

All reports are triaged on a case-by-case basis, using an internal assessment of the presented risk, and are actioned accordingly.

If your information is deemed to be actionable, preliminary enquiries will be conducted and full details sent to an identified police force to investigate them, liaising with you where appropriate.

If the victim and/or suspect are located overseas, the case will be referred to the relevant international law enforcement agency.

### Retaining Evidence

- In order for illegal activity to be investigated, retaining evidence is crucial. Be aware that retaining data should be carried in accordance with your own, legally sound internal policy.

## 4. Tell users how they can report child sexual abuse content or illegal sexual contact directly to the relevant authorities, and/or where to obtain further advice.

**The UK's Internet Watch Foundation** ([www.iwf.org.uk](http://www.iwf.org.uk)):

The IWF is the UK's hotline to combat online sexual abuse content. It is a self-regulating body working internationally with over 115 industry members, including several small and large social media providers. IWF members have access to its expertise and services, which help prevent their networks from being abused and ensure the fast removal of child sexual abuse content from their platforms.

**NCA-CEOP Report** ([www.ceop.police.uk/Ceop-Report](http://www.ceop.police.uk/Ceop-Report)):

Any illegal sexual contact/behaviour or potentially illegal activity, with or towards a child online should be reported to the NCA-CEOP Safety Centre. If a child is in immediate danger, dial '999'.

### A note on international efforts to combat child sexual abuse online

WePROTECT is a global alliance led by the UK Government to tackle child sexual abuse online. For more information on commitments made by industry, see their [Statement of Action](#).

# 5. Privacy and Controls

Privacy tools and controls are crucial for keeping young users safer when they're on your platform.

Children and young people are often excited to post personal information such as their name and contact details, or pictures and videos of what they're doing. But they need to understand that protecting their online identities and reputation is very important.

You can support their safety and privacy by providing privacy tools that keep information safe. For example, give default private settings for new users and regular reminders to be careful when sharing information online. This will also help to reassure parents and instil trust in your brand.

Over time, you can gradually introduce users to sharing more information responsibly. *(See also the advice on deeper levels of safety for under-13s and under-7s in [Section 3.](#))*

<p><b>How many children are seeing negative types of content online?</b></p>	<p>Children's knowledge and behaviour around privacy issues are mixed. Overall, children in the UK tend to claim more digital savviness than the European average</p> <p style="text-align: right;"><i>Livingstone, Haddon et al, 2014</i></p> <p>While children are generally familiar and accepting of the "rule of thumb" of not accepting strangers as friends, in reality their behaviour differs. They seem to struggle with the definitions of "stranger" and "knowing someone personally" and as a result they add people whom they have only met or seen once to their list of "friends".</p> <p style="text-align: right;"><i>Smahel and Wright, 2014</i></p>
<p><b>What techniques do they know about and use – to avoid or court risks?</b></p>	<p>Among online 12-15s:</p> <ul style="list-style-type: none"> <li>• three in ten (29%) say they have blocked messages from someone they don't want to hear from, and 52% say they know how to.</li> <li>• 15% say they have changed their social media settings to be more private, and 35% say they know how to do this.</li> <li>• 7% say they have reported something online that they found upsetting, with 29% knowing how to do this.</li> </ul> <p>On the other hand:</p> <ul style="list-style-type: none"> <li>• 11% say they have deleted history records (34% know how to)</li> <li>• 6% have amended privacy settings (24% know how to)</li> <li>• and 1% have unset filters or controls (10% know how to).</li> </ul> <p style="text-align: right;"><i>Ofcom, 2015</i></p>

## Good Practice

### 1. Limit the user information you collect, share, use and publish.

- By law, you should only collect personal data that is really needed for your web, app and mobile services. This includes name, address, age, mobile and location data. See how the Information Commissioner's Office, the UK's independent body set up to uphold information rights, defines personal [data](#), and their guidance for mobile [app developers](#).


### 2. Tell users what information you collect, why, and how long you'll keep it.

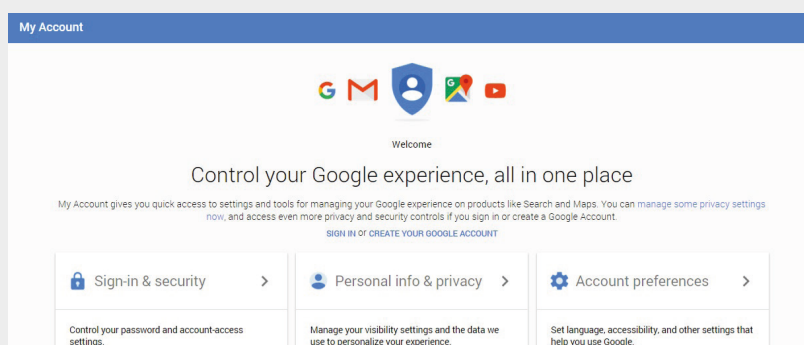
- Have a clear and accessible privacy policy, regularly signposted within your service and displayed in the safety centre (or equivalent).
- Discourage users from sharing too much personal information publicly, such as GPS location information and geotagging that can be particularly sensitive.
- Communicate in a way a young audience will understand and respond to. Use plain English, diagrams, cartoons and graphics that will appeal to them.
- In a prominent place, explain to users what others (and search engines) can see in their profile or content. Help them understand the implications of the profile settings, and use an obvious symbol - such as a lock or key - to show the secure status of their personal details.
- Highlight the kind of personal information that shouldn't be posted: for example, anything that may identify a home address, or images which contain location information, or sharing pictures of other people without asking their permission first.
- Give users regular reminders of your privacy policies, and at opportune moments. For example, when they're uploading photos or content, remind them that 'photos may not contain nudity'.

### 3. Give users the ability to see what personal information you hold about them.


- Consider if you want to let users download their data from you so that they can easily see what information you hold about them.
- Consider if this information can be downloaded in a re-usable format.
- See the ICO's [guidance](#) to help you collect and use information appropriately, and to draft a clear and informative privacy notice.

#### Examples

 Google's [My Account](#) centre allows people quick access to settings and tools that let them safeguard their data, protect their privacy and decide how their information can make Google services work better.




### Examples


 Facebook users can request a report of the data they have provided to Facebook using the “Download Your Information” ([DYI](#)) tool. This tool includes information that is also available to people in their accounts, and an Activity Log with details such as posts they’ve shared, messages and photos. It also includes information that is not available simply by logging into their account, such as the IP addresses of logs.

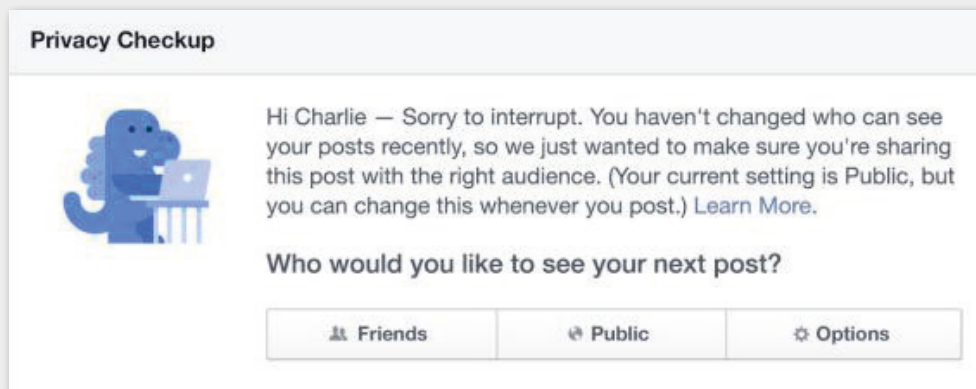
## 4. Offer privacy settings options, including privacy-by-default, to give control to your users.


- Let users adjust the privacy settings to decide with whom they’ll interact and share information. Default privacy settings can also help users be more aware of what sharing information entails – for example, ensuring that private profiles of under-18s are not searchable, or restricting access to a user’s images and content without their prior approval.
- Make sure that the privacy settings chosen by a user are applied across all your service’s tools, such as email, chat and instant messaging. If this is not possible, make sure users know where to manage the privacy settings of each tool.

### Examples

 On sign-up, users can choose to keep their Tweets private, instead of the default public settings. Protected Tweets are then only visible to a user’s approved followers. Geolocation data is set to ‘off’ by default and is only shared when a user explicitly chooses to share it with a Tweet.

 When people have chosen to post publicly for a while, they are reminded of this to make sure they’re sharing with their intended audience. When people use Facebook’s Checkup, they’ll be able to review the audience they’re posting to, which apps they’re using, and the privacy of key pieces of information on their profile. The tool is available at any time in Privacy Shortcuts.



 By default, anyone under 18 has more restrictive privacy settings. So they do not have public search listings; their email and phone number will not be set to “public”; and messages from adults who are not their friends are filtered out of the minor’s inbox. The ‘public’ audience setting is not available until they have completed extensive education around what it means to post publicly.

People who are new to Facebook now start with a default setting of “Friends” for their first post. First-time posters will also see a reminder to choose an audience for their first post, and if they don’t make one, it will be set to “Friends”.



Ask.fm allows users decide if they want to receive anonymous questions or not, or have their answers shared to other social networks. Users can “Blocklist” “contacts/friends” they don’t wish to interact with.

## 5. If you collect or use personal information about a child or young person, consider requesting consent from their parent or guardian.

See the Additional Advice in [Section 3](#) for examples.

## 6. Offer privacy tools to all your users, especially to children and young people and their guardians, and make sure they all know about them.

- Make sure users can report if their personal information is posted without consent, and that this is supported with an internal reporting process.
- Provide tools such as ‘ignore’ functions, removing people from their ‘friends’ or contact lists, and allow reviewing and removing unwanted comments from their page or wall. Consider offering users an option to approve or pre-moderate comments which may be displayed on their individual site or to restrict posting of comments to ‘confirmed friends’.
- Consider if you want to let users download their data from you, so that they can easily see what information you hold about them.

### Examples



Users can use choose “inline” audience controls to decide who can see their content. They can also review the content they’ve shared on Facebook, and content in which they’ve been tagged, such as videos and photos. People can delete the information they’ve shared; ask others to remove content they don’t like; or report content they believe violates the Community Standards or terms.



The Twitter data dashboard shows a user their account activation details, the devices that have accessed the account, and recent login history.

## 7. Get legal and expert advice to develop your privacy policy and practices on managing any data you collect, use, share and retain.

- The ICO regulates data protection and is an important resource. It has guidance on privacy, electronic communications and marketing [here](#).
- Reach out to child safety advocates, policymakers and regulators for their advice on strengthening your privacy and control solutions. See the [Annex](#) for further resources.

# 6. Education and Awareness

It is critically important to give children and young people space and opportunities where they can develop and be independent.

They can then reap the benefits of the digital age, look after themselves and their friends, and contribute positively to the wider society.

Equally, like learning about road safety or stranger-danger, online has its own set of risks that need to be taught.

You can support your young users, and their parents, schools and communities, by helping them to understand the basics. How to use your service safely, to respect the rules of the community, and to use your safety tools to their advantage.

<b>What do parents know?</b>	Three quarters of parents (75%) say they have received some type of information about helping their child manage online risks. Over half (53%) say this is from the child's school, and four in ten say it's from family or friends. <i>Ofcom, 2015</i>
<b>What do children want?</b>	Younger children are more likely to welcome parental mediation Older children are more likely to prefer to talk to their peers about the issues, feeling that parents were invading their privacy. <i>Smahel and Wright, 2014</i>
<b>Do children understand what they're being told?</b>	Information can sometimes be misleading for children, especially at younger ages. Children will "fill in the gaps" if they are asked not to do something but not given a clear reason. For example, they might think that putting personal details online means someone will come to your house and kidnap you, rather than your identity getting stolen. <i>Ofcom/ESRO, 2015</i>



## Good Practice

### 1. Use your platform to educate parents children and young people about safety.

Provide prominent and easy advice when needed to equip users to stay safe. This can be achieved in different ways:

- Provide up to date, relevant safety information that is specific to your service.
- Have a safety centre and make sure users can find it easily. All the major social media companies offer this, with tools, information and resources. For example: Facebook's [Safety page](#).
- Explain your community rules in plain language, and draw attention to them.
- Integrate safety messages into the user journey – when accepting a friend request, services updates, etc - both for new and existing users.
- Be clear how to use your safety tools such as privacy settings, reporting and blocking. Include advice on security features, such as how to create a suitable password.
- Provide review tools for existing users, prompting them to think about the settings they're using.

#### Examples



Google shows a reminder for users to review their privacy settings when using Gmail or Search.



CBBC has a "[Stay Safe](#)" hub for information on staying safe online.



Twitter uses the accounts @safety and @support, and publishes a safety blog with updates, videos and other relevant content.



The Digital Parenting Magazine is free to order [online](#) for organisations working with families.

### 2. Reach out to the community around children and young people to provide them with information, education and tools

Think of ways to reach this audience, online on your platform, offline and on third party information sites

- Make your safety centre accessible to everyone – not just members of your service. Parents can then see your steps to protect children, before allowing theirs to participate.
- Tap into school programmes run by specialist charities; get involved in Safer Internet Day every February; and engage in national policy debates by sharing your own good practice.
- Collaborate with online safety charities to create up-to-date safety messages. For example, the UK Safer Internet Centre's webpage explains the safety tools and advice of different [services](#). They have also produced printed checklists in partnership with major social media providers.
- Give links to external sources of support including helplines, law enforcement and information. They should sit in your safety centre or equivalent, and also on the reporting journey.

### Examples



Facebook has created a [Facebook Guide for Educators](#) with tips and advice on how to use Facebook within the classroom. Facebook works with the Diana Award Anti-Bullying Ambassador programme, [Think Before you Share](#). Anyone reporting bullying through a reporting mechanism is alerted to the Bullying Prevention Centre.



Ask.fm has a [Safety Centre](#) with resources developed with experts and organisations with expertise in online safety and privacy, supporting teenagers, teachers, parents and law enforcement.



Twitter gives advice for [families](#) to remind them that the service is a public space. It highlights the importance of media literacy and critical thinking when using the internet.

## 3. Work with experts to help develop your messages and to reach different communities.

Get to know online child safety experts. Working with an NGO is a good way to help young people learn from a credible voice. Seek their advice or collaboration on education and awareness initiatives. Companies work with a range of charities with expertise in bullying, self-harm (including self-harassing/bullying), suicide and general online safety issues. See the Annex for a list of relevant organisations for a list of relevant organisations.

### Examples of Organisations

The **UK Safer Internet Centre** ([www.saferinternet.org.uk](http://www.saferinternet.org.uk))



The UK Safer Internet Centre provides online safety advice and resources for young people (aged 3-19), parents and carers, teachers and child protection professionals. You can also contact the centre to suggest ideas you could contribute on Safer Internet Day.



**NSPCC** **O2/NSPCC** provide advice and guidance for parents, carers, teachers and professionals with a dedicated online safety helpline (0808 800 5002), nationwide parental workshops, parental “Share Aware” resources and PSHE accredited teacher resources, as well as a parent’s guide to social networks ([Net Aware](#)).



**NCA-CEOP**’s “[ThinkUKnow](#)” educational programme aims to empower and protect young people from sexual exploitation and abuse. Young people (aged 5-14+), practitioners and parents/carers can access a wide range of educational materials on this site, including films, factsheets, lesson plans and guidance documentation.





**Parent Zone** works with schools, parents, young people and companies to deliver effective education and awareness initiatives on issues that are caused or, more often, amplified by the internet. Working with children from 0-18, Parent Zone trains and supports the professionals who reach families to build online resilience, and develops approaches that work for multiple audiences.




**Internet Matters** is an independent, not-for-profit organisation to help parents keep their children safe online.





## Examples for Industry


 Instagram has developed its '[Parents' Guide to Instagram](#)' with Connect Safely, a US safety charity. Instagram partners with web and child safety experts worldwide to disseminate their educational materials and connect with young people who use their services.

 Facebook has worked with The Education Foundation to develop resources for teachers and also offer specific guidance in their Family Safety Centre and Bullying Prevention Centre.

An in-school and online training programme with the Diana Award on how to stay safe on Facebook has reached over 18,000 people. Facebook also sponsors Childnet's Digital Leaders Programme to build a network and online community of young people in schools who champion digital creativity and citizenship.

 Twitter speaks at events on safety and digital citizenship, and offers pro-bono advertising and best practice training support to assist digital safety NGOs to reach a wider audience. The team also regularly tweets links to NGOs, and useful resources from relevant organisations.


    Facebook, Instagram, Ask.fm and Twitter all participate at teacher and parent events to raise awareness of safety issues.

 Many charities and safety organisations have their own YouTube channel offering advice and support.





Social media companies have joined industry coalitions such as the [ICT Coalition](#), [COADEC TechUK](#) and [UKIE](#) to help promote online child safety issues more generally.


## Examples of one-stop shops for specific safety issues, such as bullying and privacy.

 Facebook's [Bullying Prevention Hub](#) has resources and guidance for young people, parents and teachers. It includes conversation starters that give advice on how to approach bullying scenarios, developed in partnership with different education experts.



 The BBC's Media Literacy programme has resources and messages to educate the public and raise awareness of children's online safety issues. Messages are tailored to children, young people, parents and carers.

 Microsoft's YouthSpark initiative partners with non-profit organisations to create bespoke resources for parents, children and teens on issues such as [sexting](#), online bullying and privacy.

 CBBC provides information on advice helplines, with links to [Childline](#), [Young Minds](#), [Shelter](#), [The Samaritans](#), [NSPCC](#), the [Anti-Bullying Alliance](#), [COAP](#) (Children of Addicted Parents and People), among others.

# Section 3:

## Under 13s - Additional Advice

Younger children need an extra level of protection, and this section includes additional advice if your service is designed for children under the age of 13.

It covers stricter user protections and should be used as complementary to [Section 2](#). Given the social and emotional developmental differences within this age band, we also include additional advice to protect the under-7s.

Platforms for under-13s are typically walled garden experiences to ensure a high level of safety. The examples included here are based on services across a range of ages: Moshi Monsters and PopJam, Disney Club Penguin, CBeebies online and CBBC online.

### *A note on moderation*

In this guide, ‘pre-moderation’ refers to content reviewed by a service provider before it becomes visible to others. ‘Post-moderation’ is reviewing after content has been posted, and any action taken to remove inappropriate content and warn or ban users who break the rules.

‘Reactive moderation’ refers to moderation that takes place only after a report has been made. ‘Reporting mechanisms’, or reports submitted by users, are regarded as a reactive moderation tool in this guide.


## Principle 1 - Content


The following approaches are examples of good practice to ensure the content on your site is suitable for under-13s, and to restrict access to content that might be inappropriate for them.

### 1. Use suitable language and messages for your target age group.

You're talking to young children, so deliver clear and simple messages in their own vocabulary, and repeat them throughout the user journey.

**Examples**

 Club Penguin's content rules are clear and succinct:



The screenshot shows a dialog box titled "Club Penguin Rules" with an orange background. It lists four rules, each with an icon: "Respect others" (smiley face icon), "Chat nicely" (speech bubbles icon), "Stay safe online" (lifebuoy icon), and "Play fair" (game controller icon). Each rule includes a brief description. At the bottom of the dialog is an "Ok" button.


### 2. Offer a walled garden environment for younger children.


As a safe place to play and communicate, a closed setting is best for the youngest children (for example, under 7).

Designing this involves limiting or restricting content generated from third parties on your service; pre-moderating, limiting or restricting communications such as message boards and emails between members; and creating a limited range of messages or images within communications (e.g. canned responses such as "well done!").

As children get older and familiar with your service, they can benefit from a gradual exposure to features such as exchanging messages, learning to be responsible and knowing what to share safely.

**Examples**

 CBeebies is a walled garden site, designed for children to use with their parents or carers. All content is specifically targeted at under-7s, and the only links outside the site are from the "Grown-ups" support area to similar support sites, and to specifically approved third party sites of the TV independents responsible for the programmes. These links are pre-vetted by staff to comply with BBC Editorial Guidelines.

 PopJam labels content for all YouTube videos that are rated 13+. They have their own rating system and will restrict YouTube videos if they consider they are not appropriate for under-13s.

### 3. Consider a mix of moderation styles for all content.

With a robust in-house system, you can pre-moderate before content is posted, post-moderate once content is shared (e.g. checking that content remains suitable), and apply reactive moderation to investigate promptly any user reports you receive.

Depending on your scale and service, you can achieve this with a blend of manual and automated solutions, both of which can also be outsourced to specialist companies. For example, you might want to use a software solution to run keywords to identify inappropriate words, but manually approve comments before their publication (pre-moderation).

Reactive moderation (moderation after a report, usually by a user) is covered under Principle 3 of this section.

#### Examples



Moshi Monsters uses a moderation tool called CRISP™ to make their moderation scalable, efficient and affordable. They also employ professional human moderation companies to help them deal with global users across time zones.



CBBC's message boards have automatic filters, are pre-moderated and have community hosts. At the point of posting, the filters block non-CBBC URLs, email addresses and inappropriate user names and messages. Each message is checked before it is published, and moderators will also spot and flag suspicious users, as well as users in distress. A team of public-facing community hosts acts as the first point of contact for the moderators when they have concerns about a user.



Disney Club Penguin uses various pre- and post-moderation tools:

- A sophisticated chat filter blocks inappropriate words and phrases before they can be viewed by other players (so pre-moderation);
- Reporting tools allow players to report any misconduct to a team of moderators (reactive moderation); and
- In-house moderators monitor online activity and review any reports (post-moderation and reactive moderation).

### 4. Grown-ups have an important role to play when users sign up to your service.

Parents can be contacted directly to make sure the age of users is correct, or you can use third party verification systems such as AgeCheq. Parents can also be important allies in helping children understand and abide by the rules over time.

**Disney Club Penguin** involves parents from the beginning, asking for a parent's email address as part of the registration process. He or she needs to activate their child's account to verify and complete the registration process. Parents can also create a Parent Account to manage their child's Club Penguin experience.

### 5. Become familiar with the UK rules on online advertising to children.

Several sections of the [UK Advertising Code](#) contain rules relating specifically to children, including prohibited advertising of age-restricted products such as alcohol, gambling and electronic cigarettes. Make sure you are up to date on the mandatory UK advertising rules and that you understand how they are applied online, as well as to email and direct marketing generally. For more general information on advertising regulation visit the websites of CAP ([www.cap.org.uk](http://www.cap.org.uk)) and the ASA ([www.asa.org.uk](http://www.asa.org.uk)).

## 6. Children and young people find smart ways around your content moderation, so review your approaches.

For example, content filters may not pick up that users have created synonyms such as 'chair' to insult others; a human moderation team can help spot them.

### Principle 2 - Parental controls

It's important to stay in touch with parents and guardians: younger children are often supervised and you can offer tools and information to support grown-ups' approaches to online safety.

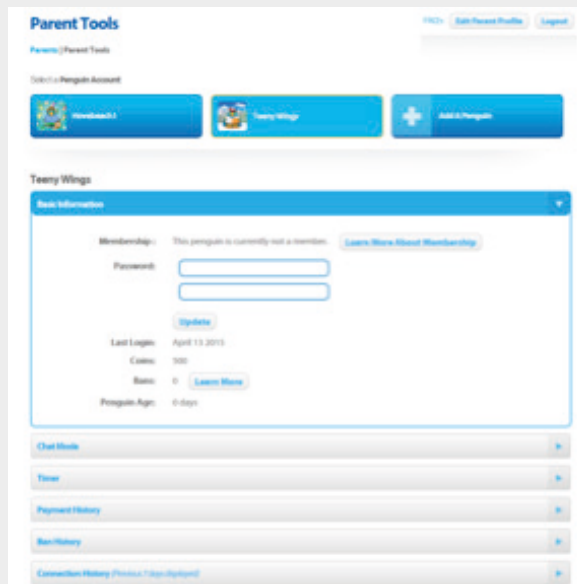
#### Examples



Their home page has a Parental Lock page explaining how to switch this control on and off.



Parent-controls include the ability to set a timer to decide when and for how long a child can play; update passwords; change the chat mode; cancel a membership; and view a child's playing history (their login history and any ban



### Principle 3 - Dealing with abuse/misuse

Even though your audience may be young, and even in pre-moderated environments, abuse and misuse will happen. Be prepared for it, and ready to help and educate your users.


#### 1. Inappropriate behaviour needs warnings in clear and understandable language.

Be clear about the consequences if users persist in disregarding your rules.

#### Examples



Depending on the severity of the offence, any player found breaking the rules will typically be issued first with warnings, or temporary bans from play. Ultimately, they can lose their accounts.

 Minecraft blocks specific features for players under 13 playing on Minecraft Realms, such as chatting in Scrolls, making purchases or changing settings on the [Mojang account site](#).

## 2. Actively manage your community, complementing the areas that pre-moderation alone can't address.

### Examples



Community hosts play an important role in preventing cyber bullying. They are alert to the signs and help make the communities welcoming and inclusive by discouraging exclusive clubs and cliques.

It can be difficult to spot a subtle pattern of bullying when, as moderators do, you are looking at individual messages, out of context in the moderation system. So it is the hosts who play a vital part in being across all the various discussions. They can identify troublemakers and, conversely, users who are in danger of being isolated.

CBBC also aims to minimise the potential for grooming online. It restricts message boards by age, reverts to limited text functionality in games where moderation isn't available, and keeps moderators aware of the latest grooming techniques.

## 3. Try to make your responses constructive and positive.

### Examples




At Moshi Monsters, moderators consider two key questions before taking any action: 'What is the intention of the content/post?', and 'what is the context of the situation?' Users are given the benefit of the doubt. A good moderator will not escalate any situation; instead, they should defuse a potential problem. The most effective way of dealing with abuse and misuse is to point out alternative behaviour, and educate users why something isn't permitted. Their message is 'smile from the wrists down'.



If unacceptable behaviour occurs, these platforms may restrict users to viewing (but not posting) content, before deciding whether to hide or ultimately delete user accounts. This is intended to educate users about the consequences of misbehaviour.



Both Moshi Forums and the PopJam app use a trust system that identifies every user as ‘trusted’, and their ability to view, post and participate is influenced by their user trust score. The higher the score, the more they are trusted, and they don’t require pre-moderation. The lower the score, the less freedom they have. Low scorers’ content goes into ‘pre-moderation’ and must wait for a moderator to manually review and approve their posts.

 Suspensions are unusual as a user must have demonstrated malicious intentions. However, when they do occur, a user can lose not only the work they created but their community following, so the consequences can be painful. The account owner or a parent must then contact the Customer Services group to reactivate the account.

#### 4. Refresh training on understanding children and young people, especially regarding online safety and child protection.

In addition, all staff in direct contact with children should have their criminal record checked against the Conduct a Disclosure and Barring Service (DBS) in the UK.

##### Examples



CBBC’s trained moderators read every message before it is published. They refer anything that asks for help, or which hints at a child being at risk, to the CBBC child protection lead.

Situations may include extreme bullying, eating disorders, self-harm, domestic violence, depression, sexual or physical abuse, or potential grooming. If a child posts a message directly asking for help, or is troubled, a BBC staff host will post a reply from a list of ‘distress responses’, which cover scenarios ranging from having an eating disorder to domestic violence.

These responses have been developed with leading children’s charities such as ChildLine and Childnet International and were revised with the help of trained counsellors. CBBC also works closely with a children’s psychologist and counsellor who give in-depth public (and, where necessary, private) help to children who need it.

#### 5. Inform and contact grown-ups to safeguard children in their care.

As well as getting parents involved at a child’s registration stage, stay in touch with them – for example, when you change your terms of service or add a new feature that involves social interaction. Younger children in particular can be more vulnerable to abuse and misuse, whether as a victim or as a perpetrator. Knowing how to contact a parent or guardian can be helpful in these cases. You can also supply a dedicated email address for parents to make sure that they can reach you directly.

##### Examples



Moshi Monsters offers parents support through email ([parents@mindcandy.com](mailto:parents@mindcandy.com)) and phone to control their children’s apps and accounts online.



Parents and players can contact a guest experience team via phone or email ([support@clubpenguin.com](mailto:support@clubpenguin.com)). All feedback is recorded and summarised into a weekly report, with key themes and recurring comments discussed internally. All moderators’ work is monitored and reviewed every week to ensure a consistently high quality of service. The guest experience policies are also reviewed regularly.

## Principle 4 - Reporting child abuse or illegal sexual contact

If you come across child abuse content or child sexual contact on your site, it is your responsibility to report it.

Do not attempt to deal with it yourself. Depending on its nature, report the issue to the experts at either the IWF or CEOP. See [Section 2](#), to find out which organisation you should approach.

However, if you believe a child might be in danger, call 999 immediately.

## Principle 5 - Privacy and Control

### 1. Base your user privacy measures on age. Many platforms give under-13s enhanced protections.

You might want to restrict user generated content (UGC), text uploads or information exchange until you have verified the account with an adult to check the user's age.

You might also look to streamline user registration by avoiding collecting email addresses, if they're not needed to use your service.

#### Examples



On Moshi Monsters, users can create a limited account with restricted social features. To lift this restriction, parents must verify the account; this is enabled when users give a parent's email address and select their country of residence. The parent then receives an email with the user's information, including the password for the account, and is asked to confirm the details. They can also request to have social features such as forum interaction switched off, and also 'unfriend' anyone on their child's 'friends tree'.



Club Penguin does not allow profiles with personal information. Until a username is approved by a moderator, a player is identified as an ID number. If a username is rejected, players can choose another name. In addition, chat filters are designed to prevent any personal information from being shared.



### 2. Educate young users about privacy, and how to preserve it.

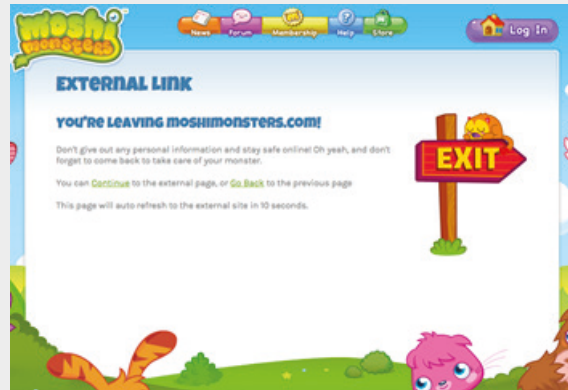
Your site may be a user's first introduction to the importance of online privacy. In their own language, help them to understand how to be responsible about their data. Also offer information and advice when they share information with other users.

## Examples

**BBC** On BBC services, children are encouraged to ask for their parents'/carers' permission before creating a user account, and to make sure their parents know they will be using the message boards.



Before redirecting users to external sites, Moshi Monsters reminds them to stay safe by not giving out personal information online:



### 3. Children's data is sensitive – get legal advice.

There are laws about the collection, use and retention of children's personal information. For example, if you run competitions for under-18s, entrants must have parental permission.

'Data' can include all types of content, including photographs. Generally speaking, the less data you collect, the fewer compliance issues you will face. The [Annex](#) points to some key legislation you should know. See also [Principle 5](#): Privacy and Control.

## Examples

**BBC** Children's data is regarded as sensitive and is given the highest priority in terms of information security. It is never supplied to third parties without consent and is not used for commercial marketing purposes. The BBC's privacy policy applies to all children's sites.



Data collected is only used for internal marketing, and parents can opt out of this at any time. Data will also be deleted on request, including pinboard messages, login and time stamp information, IP addresses associated with the account and user profile information. The privacy policy is posted throughout the site and included in the parent registration request email.



When children are invited to send their own content the platform always supplies a link to the Terms of Use and a recommendation that a parent or guardian checks them before giving their consent. They also advise users not to include any personal information in their submission, and only send in their own original content (not someone else's). All UGC submitted is individually reviewed by a human moderator before being published, to make sure it is appropriate for all audiences and does not include personal information.

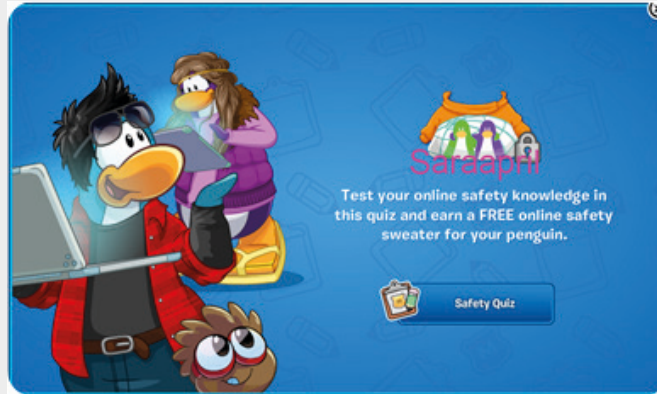
## Principle 6 - Education and Awareness

The advice for this Principle in [Section 2](#) also applies here. Importantly, tailor the language, educational messages and approaches in a way a young user can follow.

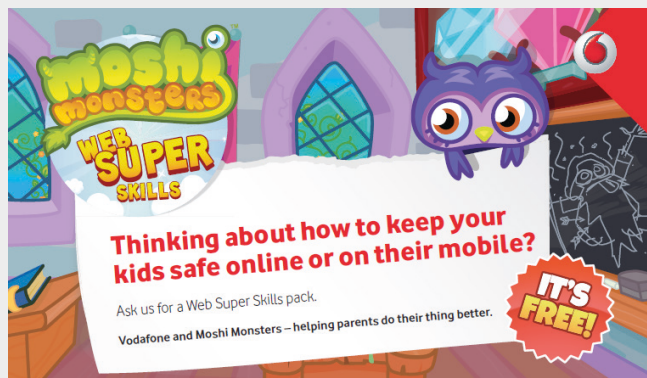
### Examples



Disney Club Penguin conducts an “It Starts With You” campaign on online safety to encourage children to spread positive behaviour. This includes tips for parents and children, and an online safety quiz in the virtual world:



Moshi Monsters has developed activity cards with The Vodafone Foundation to help parents educate children about online safety:



CBBC includes information with helplines and advice for children:



# Annex

In this section we include reference material on areas of prime importance to any operator with a platform:

1. Legal Landscape. A summary of key UK legislation
2. Child Development Chart. How children and their attitude to risks evolve throughout childhood
3. Evidence Section: Social media risks research
4. Examples of Tools Used by Social Media and Interactive Services
5. Contacts and Links

# 1. Legal Landscape.

## A summary of key UK legislation

Below, we highlight some of the important legislation that affects every platform operator.

Please note that this guidance is not a substitute for professional legal advice.

### UK Civil Law

#### Data Protection Act 1998

If you collect and process personal information, you must comply with eight principles of the Data Protection Act. These make sure that personal information is:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than is necessary;
- Processed in line with individuals' rights;
- Secure; and
- Not transferred to other countries without adequate protection.

By law, you should only collect personal data that is really needed for your web, app and mobile services. Personal information includes name, address, age, mobile and location data. See how the Information Commissioner's Office, the UK's independent body set up to uphold information rights, defines personal data, and their Guidance for mobile [app developers](#).

#### Defamation Acts 1996 and 2013

Defamation is a civil wrong which is partly governed by the "common law". However, the Defamation Acts of 1996 and 2013 contain a number of provisions, primarily in relation to defences. The law on defamation applies to any material which seriously harms the reputation of an individual or an organisation, and it includes material published on the internet. A civil action for defamation can be brought by an individual or a company, but not by a public authority. It is up to the claimant to prove that the material is defamatory. However, the claimant does not have to prove that the material is false – the burden of proof on that point lies with the author/publisher who, if they wish to rely on a defence of truth, has to prove that what they have written is true or substantially true.

The 2013 Act introduced a requirement that for a statement to be defamatory the claimant must show that the publication of the statement has caused, or is likely to cause, serious harm to his or her reputation. In the case of bodies trading for profit the serious harm test will only be met if the body can demonstrate actual or likely serious financial loss. The Act also created new statutory defences of honest opinion and truth to replace the existing common law defences, and a new statutory defence for publications in the public interest.

If defamatory material is posted on your website, the person affected can inform you of its contents and ask you to remove it. The 2013 Act provides a defence to website operators who, on receipt of a complaint, follow a process aimed at enabling the complainant to protect their reputation by resolving matters directly with the person who is responsible for the defamatory posting. Where the person

responsible cannot be identified or is unwilling to engage in the process, the website operator must remove the material or forfeit the defence (in which case they can be sued for defamation).

Where the person responsible for posting the material can be identified, the person affected can sue him or her for defamation. The person affected may also be able to obtain a court order (an injunction) to require removal of the material against either the person responsible for the posting or the website operator.

The 2013 Act applies to England and Wales only, although new defences relating to scientific and academic journals and conferences also apply to Scotland. Various provisions of the 1996 Act extend to both Scotland and Northern Ireland.

## **The Regulation of Investigatory Powers Act 2000 and the acquisition of communications data.**

The Regulation of Investigatory Powers Act 2000 (RIPA) provides the main legal framework for governing the use of investigatory powers, including the acquisition of communications data and the interception of communications. In relation to child internet safety, social network providers and other communications services providers are most likely to come into contact with RIPA when they receive a notice requiring the disclosure of communications data under Chapter II of Part I of RIPA. Such a notice can only be issued to a communications service provider where necessary and proportionate to do so for a specific statutory purpose, such as for the purpose of preventing or detecting crime or of preventing disorder.

Further details, including definitions of communications service providers and communications data can be found in the Acquisition and Disclosure of Communications Data Code of Practice 2015.

Communications service providers can also be required to retain communications data under the Data Retention and Investigatory Powers Act 2014. Before such a requirement can be placed on a provider the Secretary of State must take reasonable steps to consult the relevant provider. Further details can be found in the Retention of Communications Data Code of Practice 2015.

On 4 November 2015 the Government published the draft Investigatory Powers Bill. This Bill consolidates a number of investigatory powers, including powers to acquire and retain communications data. Following pre-legislative scrutiny the Government intend to introduce the Bill to Parliament in spring 2016 and for it to come into force before the end of 2016.

## **UK Criminal Law**

It is important to note a general principle: an action that is illegal if committed offline is also illegal if it is committed through an interactive online service.

This applies for instance to issues such as distributing illegal material and to harmful behaviour if it amounts to a course of harassment, or grooming.

Anyone encouraging or assisting another to commit an offence is liable to be tried and punished as though they themselves committed the offence in question.. Equally, there are offences which apply to those who encourage or assist others to commit an offence even if that offence does not in fact take place. Those who conspire or attempt to commit an offence will also be held liable.

An offender is equally liable if any of the above behaviour takes place through a computer or mobile device.

Other criminal activity may include fraud and identity theft.

Each case will be different, and no guide such as this can set out a definitive explanation of the law.

All the Acts mentioned below can be found in full at [www.legislation.gov.uk](http://www.legislation.gov.uk)

## **Communications Act 2003 (UK)**

Section 127 (1) provides that it is an offence if any person sends a message which is grossly offensive, indecent, obscene or menacing by means of a public electronic communications network, or if a person causes any such message or matter to be sent.

Section 127 (2) provides that a person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he sends by means of a public electronic communications network a message he knows to be false, causes such a message to be sent, or persistently makes use of a public electronic communications network.

The offences carry a penalty of a maximum of six months' imprisonment and/or a level five fine.

## **Computer Misuse Act 1990 (*applies UK wide*)**

The following offences could apply in relation to social media use under the Computer Misuse Act (CMA):

Section 1 creates an offence of unauthorised access to computer material or data, which includes using someone's password without their permission and hacking into someone else's account or computer. Section 1 carries a maximum of two years' imprisonment.

Section 2 creates an offence of unauthorised access with intent to commit or facilitate commission of further offences. This could include someone hacking into someone else's social media account and then going on to commit offences which could include posting offensive material or bullying. Section 2 carries a maximum of five years' imprisonment.

Section 3ZA creates an offence of unauthorised acts causing, or creating risk of, serious damage, and is designed to address the most serious cyber-attacks; for example, on essential systems controlling power supply, communications, food or fuel distribution. A major cyber-attack of this nature could have a significant impact, resulting in loss of life, serious illness or injury, severe social disruption or serious damage to the economy, the environment or national security. The use of social media could play a part in carrying out such an attack. Where the unauthorised act results in serious damage to human welfare or to national security, the maximum sentence is life imprisonment. Where the unauthorised act results in serious damage to the economy or the environment, the maximum sentence is 14 years' imprisonment.

Section 3A creates an offence of making, supplying, or obtaining an article (e.g. 'hacking tools') intending it to be used to commit, or to assist in the commission of, an offence under sections 1, 3 or 3ZA of the CMA. This could apply to the use of apps and other tools that could be used to commit an offence – for example an app that allows you to stalk a partner. Section 3A carries a maximum of two years' imprisonment.

## **Malicious Communications Act 1988**

Section 1 of this Act makes it an offence to send any letter, electronic communication or other article to another person that is indecent, grossly offensive or which conveys a threat or information which is false and known to be so by the sender,, with the intention that it should cause distress or anxiety to the person who receives it, or to any other person to whom the sender intends that it or its contents or nature should be communicated.

The offence is subject to a maximum 2 years imprisonment.

Section 2 refers to corresponding legislation made under the Northern Ireland Act 1974.



## Obscene Publications Act 1959

Publication of obscene articles is an offence under section 2 of the Obscene Publications Act 1959 (OPA). The OPA applies equally to material published in hard copy, over the internet, or broadcast on television. The maximum penalty for an offence under the OPA was recently raised from three to five years' imprisonment. The test of obscenity – a tendency to deprave or corrupt those likely to read, see or hear it - is flexible, allowing the courts to reflect society's attitudes towards pornographic and other material. It is possible therefore that material found to be 'obscene' by the courts many years ago may not be prosecuted today.

The OPA also includes a "public good" defence where publication of the article in question is justified as being for the public good on the ground that it is in the interests of science, literature, art or learning, or of other objects of general concern.

## Indecent photographs and pseudo-photographs/ prohibited images of children

The **Protection of Children Act 1978** ("the 1978 Act") essentially prohibits creation or distribution of indecent photographs or pseudo photographs (images which appear to be photographs) of children, in whatever form. The proscribed activities are taking, making, permitting to be taken or made, distribution or showing, possessing with intent to distribute, or publish or cause to be published an advertisement for such photographs. The maximum penalty is ten years' imprisonment. Encouraging or assisting the making of indecent images could also be charged, for example where an adult is coercing a child to self-produce indecent photographs even where no image is in fact produced.

Simple possession of such a photograph is an offence under section 160 of the Criminal Justice Act 1988, and carries a five year maximum penalty.

Under Section 62 of the Coroners and Justice Act 2009 it is an offence to possess "prohibited images" of children (certain types of pornographic non-photographic images of children i.e. cartoons and computer-generated images). This carries a three year maximum prison sentence. Their publication or distribution could also constitute an offence of publishing an obscene article under the Obscene Publications Act 1959 (maximum sentence five years); the Obscene Publications Act applies equally to material published in hard copy, over the internet, or broadcast on television.

Although there are defences specified in the above Acts, it is unlikely that any of these could apply to images that might be sent over a public interactive service, so anything discovered in the course of moderation which appears to be an indecent photograph, pseudo photograph or prohibited image of a child needs to be reported and properly investigated.

A defence to "making" an indecent photograph of a child is provided by section 1B of the 1978 Act for certain professionals who have found it necessary to make such an image for the purpose of prevention, detection or investigation of crime.

A Memorandum of Understanding (MoU), between the Crown Prosecution Service and the Association of Chief Police Officers (now the National Police Chiefs' Council), addresses the handling of illegal images by a range of professionals included those involved in IT.

The key points covered by the Memorandum are:

- It is an identified role;
- The speed at which the illegal image is reported and any delay was reasonable; and
- The handling and storage was appropriate and secure.

Further information on the MoU is available on the CPS website, [www.cps.gov.uk](http://www.cps.gov.uk) and the IWF website [www.iwf.org.uk](http://www.iwf.org.uk).

Section 8 of the 1978 Act refers to corresponding legislation made under the Northern Ireland Act 1974.

## Protection from Harassment Act 1997

The Protection from Harassment Act 1997 captures wide range of behaviours, including harassment, and stalking. The Act makes it an offence for someone to pursue a course of conduct which amounts to harassment or stalking or causes someone to fear that violence will be used against them.

Section 2 of the Act makes it an offence for someone to pursue a course of conduct which the perpetrator knows, or ought to know, amounts to harassment. Harassment is generally understood to involve improper, oppressive and unreasonable conduct that is targeted at an individual and calculated to alarm them or cause them distress. This offence is summary only and carries a penalty of a maximum of six months' imprisonment and/or a level five fine.

The more serious offence, in section 4 of the Act, is committed when a person pursues a course of conduct which causes another to fear, on at least two occasions, that violence will be used against them, and the offender knows, or ought to know, that the conduct will cause the other so to fear on each occasion. It carries a penalty of a maximum of five years' imprisonment and/or an unlimited fine.

Under section 2A of the 1997 Act it is an offence to pursue a course of conduct that amounts to stalking, and section 4A makes it an offence to do so in a way which causes another person to fear, on at least two occasions, that violence will be used against them, or causes severe alarm or distress which has a substantial adverse effect on the person's usual day-to-day activities.

Under section 5 of the 1997 Act, a court sentencing someone convicted of any offence may also, to protect a victim from harassment or fear of violence, impose a restraining order prohibiting specified forms of behaviour. Under section 5A of the Act, a restraining order may similarly be made on acquittal. Breach of a restraining order is a criminal offence punishable by up to five years' imprisonment.

In addition to these criminal offences, section 3 of the Act provides a civil remedy which enables a victim to seek an injunction against a person who is harassing them or may be likely to do so. There is no need for a person to have been convicted of harassment in order for an injunction to be granted against them.

Section 13 refers to corresponding legislation made under the Northern Ireland Act 1974.

## Public Order Act 1986

Section 5 makes it an offence to use threatening or abusive words or behaviour, or disorderly behaviour, within the hearing or sight of a person likely to be caused harassment, alarm or distress thereby. Section 5 further sets out that it is an offence to display any writing, sign or other visible representation which is threatening or abusive within the hearing or sight of a person likely to be caused harassment, alarm or distress thereby.

Possession of racially inflammatory material with intent to share it is prohibited by section 23 of the same act.

This offence may apply where a mobile phone is used as a camera or video, and images are then transmitted.

The **Racial and Religious Hatred Act 2006** and **Criminal Justice and Immigration Act 2008** added provision for the same offences in relation to when stirring up religious hatred or hatred on the grounds of sexual orientation respectively where such a stirring up is intended.

## Sexual Offences Act 2003

The key legislation in this area is the Sexual Offences Act 2003 (the “2003 Act”). This Act includes both specific offences against children, as well as other offences which may be committed against both adult and child victims.

Many of the offences in the Act require physical contact, however conspiracy to commit, and encouraging or assisting the commission of such offences can be carried out online.

The Act includes the offences of rape (which includes penile penetration of the mouth and anus), assault by penetration and sexual assault (i.e. sexual touching) in sections 1 to 3 respectively. These offences may be committed against both adult and child victims, but are only committed where the victim does not consent to the activity, and the perpetrator does not reasonably believe that the victim consents. Rape and assault by penetration carry a maximum life sentence; sexual assault a maximum sentence of ten years’ imprisonment.

Section 4 creates an offence of causing a person to engage in sexual activity (to which they do not consent). Where the conduct involves penetration, this carries a maximum life sentence, otherwise the maximum is ten years.

### ***Offences against a child under 13***

Sections 5-7 create the offences of rape, assault by penetration and sexual assault on a child under 13, and section 8 creates the offence of causing a child under 13 to engage in sexual activity. The crucial difference from the offences in sections 1-4 is that if the relevant penetration or touching took place then an offence was committed; absence of consent need not be proved. The maximum sentence for sexual assault and for causing or inciting a child under 13 to engage in sexual activity not including penetration is also higher (14 rather than 10 years).

### ***Offences against a child under 16***

The offences in sections 9-15 apply to any complainant under 16; it would be more usual to charge one of the ss 5 to 8 offences if applicable where the complainant is under 13, unless there is some doubt about the age. The offences in this category cover sexual activity with and involving children with the intention of protecting children from engaging in or witnessing sexual activity.

Section 9 creates the offence of sexual activity with a child and section 10 of causing or inciting a child to engage in sexual activity. These offences both also carry a maximum sentence of 14 years. Absence of consent need not be proved. The section 10 offence could be used, depending on the circumstances, to prosecute those who encourage or pressurise children to indulge in sexual activity online or self-create indecent photographs, or who arrange for sexual offences to be committed against children so that they can view the activity remotely for their own gratification.

Sections 11 and 12 create offences of, respectively, engaging in sexual activity in the presence of a child, and causing a child to watch a sexual act, for the sexual gratification of the offender (see *R v Abdullahi* [2006] EWCA 2060 where this term is given a wide meaning and includes future as well as immediate gratification). The sexual gratification of the offender is an important qualification given the wide definition of sexual activity which otherwise could criminalise adults kissing in front of children or allowing them to watch rated videos suitable for their age. These offences can be committed by anyone above the age of criminal responsibility. These offences both carry a maximum sentence of ten years if tried on indictment. These offences could apply also where the child views the activity remotely, for example via web cam.

Lower maximum sentences for the above offences against a child apply where the perpetrator was also under 18.

Section 14 creates a preparatory offence of arranging or facilitating the commission of one of the

above offences, again with a maximum sentence of 14 years. This can be committed by anyone regardless of their age.

Section 15 creates another preparatory offence of meeting a child following sexual grooming. This applies where an adult has communicated with a child under 16 (whom they do not reasonably believe to be 16 or over) on at least one occasion (reduced, in April, from two occasions - Criminal Justice and Courts Act 2015) and then meets, or travels or arranges to meet, the child (or the victim travels with the intention of meeting the adult) with a view to committing a sexual offence. It carries a maximum sentence of ten years and can only be committed by a person over the age of 18.

Specific, similar child sexual offences to those outlined above apply where the activity involved the abuse of a position of trust (for example in a school, hospital or children's home), or took place within the family.

The Act also creates offences relating to the sexual exploitation of children (until earlier this year, "child prostitution and pornography") offences. These include paying for the sexual services of a child, causing or inciting the sexual exploitation of a child, controlling a child in relation to sexual exploitation and arranging or facilitating the sexual exploitation of a child. These offences apply where payment is made to the child or a third person in return for the sexual activity, or where an indecent image of the child is recorded. They carry a maximum sentence of 14 years, except for paying for sexual services including penetration from a child under 13, which carries a life sentence.

Section 72 of the 2003 Act provides for extra-territorial jurisdiction for sexual offences against children. Where a UK national does an act outside the UK that would constitute an offence if carried out in England and Wales, the UK national is guilty of that offence in England and Wales. Where a UK resident does such an act, and where that act is also an offence in the country where it took place, the UK resident is guilty of the offence in England and Wales.

See also the [Sentencing Council's Definitive Guide on sexual offences](#).

## **Suicide Act 1961**

Under section 2(1) of the Suicide Act 1961 it is an offence to carry out an act capable of encouraging or assisting the suicide or attempted suicide of another person with the intention to so encourage or assist. The law applies to online actions in exactly the same way as it does offline. The person committing the offence need not know the person encouraged or assisted, or even be able to identify them, and may be prosecuted whether or not a suicide or attempted suicide takes place.

The maximum penalty for an offence under section 2(1) of the 1961 Act is 14 years' imprisonment.

There are equivalent provisions in section 13 of the Criminal Justice Act (Northern Ireland) 1966 (which was amended by section 60 of the Coroners and Justice Act 2009 in the same terms as the Suicide Act 1961 was amended by section 59). The crime of assisted suicide does not apply in Scotland: the matter is dealt with there as culpable homicide, on a case by case basis, depending on the particular facts and circumstances.

## **Serious Crime Act 2015: New offences**

The Serious Crime Act created a new child sex offence:

Possession of a paedophile manual, which came into force on 3 May. This criminalises the possession of material which provides advice and guidance on how to abuse children sexually and carries a maximum sentence of three years.

## Legal basis for law-enforcement action on terrorist material online

1. Under UK legislation, 'terrorist' material includes information which would be useful for committing an act of terrorism e.g. bomb making instructions contained in Inspire magazine (sections 57 + 58 of TACT 2000) or content which glorifies/encourages an act of terrorism e.g. the Al-Shabaab video 'An eye for an eye' (sections 1 + 2 of TACT 2006).
2. The UK police Counter Terrorism Internet Referral Unit (CTIRU) refer terrorist content that it has identified to social media companies and requests that it is taken down. The public can also refer content directly to Communications Service Providers or through the CTIRU website.
3. Industry cooperation is on the basis of a voluntary arrangement between CTIRU and industry. While there is provision in UK law for the police to issue a notice and take down order where unlawful content is hosted in the UK, this is rarely used.
4. Social media companies assess the content against their own terms of use and remove it if it breaches those terms. Whilst law-enforcement requests are considered alongside other user and public notifications most companies will prioritise requests from law-enforcement or known 'super-users' with a track record of assessments in line with their own policies. Where companies take action this removes access to the content from the whole platform, not just for users accessing it from within a particular jurisdiction.

## US Law

### COPPA

The Federal Trade Commission, an independent agency in the United States for the protection and promotion of consumers, enforces the Children's Online Privacy Protection Act (the 'COPPA' Rule). It applies to the online collection of personal data from online services, including apps, that are directed to children under 13 years old.

The FTC defines Personal Information and Verifiable Consent as the following:

**Personal information** (PI) or personally identifying information (PII) is defined by COPPA as: collecting personally identifying information online including but not necessarily limited to: full name, address, email address, telephone number, persistent identifiers that can be used to recognize a user over time and across different Web sites or online services (e.g., IP address, DUID or device ID, etc.) photographs, or any information that can lead to identifying, locating and contacting a child. Information collected through cookies or other types of tracking systems are included in the definition of "personal information."

**Verified Parental Consent** (VPC) is required to collect personal data from children. It comes with specific exceptions for data collection for specific purposes. The main exception being that collection of PI is allowed without VPC for support for the internal operations of the Web site or online service means.

For more information on the COPPA Rule, the FTC has a six-step [guide for compliance](#), a list of [FAQs](#), [guidance](#), and an email address for enquires ([CoppaHotLine@ftc.gov](mailto:CoppaHotLine@ftc.gov)). The FTC has also approved providers of Safe Harbor to support with COPPA compliance: ESRB, TRUSTe, CARU, PRIVO, KidSAFE and iKeepSafe.

## 2. Child Development Chart.

### How children and their attitude to risks evolve throughout childhood.

This chart summarises the development of children at various ages from 3-18: how they see themselves, their priorities, their behaviour online and their attitude towards risk.

Source: Dr. Angharad Rudkin, Chartered Clinical Psychologist, University of Southampton

<b>3 – 5 year olds</b>		
<b>Overall development</b>	<b>Key online activities</b>	<b>Attitudes to risk</b>
<p>They can put themselves in others' shoes, but they are still quite fooled by appearances.</p> <p>Beginning to learn that there are social rules to follow.</p> <p>Starting to build up friendships but peer pressure remains low.</p>	<p>Entertainment, particularly games and TV.</p>	<p>They may be unaware of risks.</p>
<b>6 – 9 year olds</b>		
<b>Overall development</b>	<b>Key online activities</b>	<b>Attitudes to risk</b>
<p>Play is mainly pretend/role-play, moving towards greater rule-based reality play. Becoming socially more sophisticated; the need to fit in and be accepted by the peer group becomes more important.</p> <p>Learning how to manage their thinking and their emotions. Learning about the complexities of relationships; if they can't manage these it can lead to alienation, bullying and loneliness. At around 7, they undergo a significant shift in thinking to more order and logic.</p> <p>They are now frequent users of the internet but with limited information on staying safe online, which may make them vulnerable.</p>	<p>Entertainment and fun – games, films, TV, video.</p> <p>Communications largely with family only</p>	<p>Children largely compliant with messages from school/home – although if risks aren't explained clearly, they imagine their own explanations.</p>
<b>10 – 13 year olds</b>		
<b>Overall development</b>	<b>Key online activities</b>	<b>Attitudes to risk</b>
<p>Moving towards more adult ways of thinking but still not making decisions the way adults would.</p> <p>Very aware of social pressure and expectations; will change aspects of themselves in order to fit in and be accepted by peers. Friends are becoming more important.</p> <p>More aware of what's 'cool' or not, including brands.</p> <p>Girls show a decrease in self-esteem as they compare themselves to others around them.</p>	<p>Communications with friends; games (for boys), gossip, TV/films, shopping.</p> <p>Open communication across a range of sites.</p> <p>Visual communication becomes key.</p> <p>Development and honing of self-image.</p>	<p>Developmentally, the strong desire for immediate rewards triggers risk-taking behaviour.</p>

<b>14 – 18 year olds</b>		
<b>Overall development</b>	<b>Key online activities</b>	<b>Attitudes to risk</b>
<p>Underdoing significant neuro-psychological changes, leading to differences in the way they perceive emotions and make decisions. Developments in the pre-frontal cortex may contribute to the increase in risk-taking behaviour seen during adolescence.</p> <p>Mental health difficulties such as anxiety and depression can intensify.</p> <p>Still have difficulties realising that others can have a different perspective, so may find it hard to work out interpersonal problems.</p> <p>Adolescence is a time characterised by idealism, with a tendency towards all-or-nothing thinking.</p> <p>Highly dependent on peers for a sense of well-being. They need to feel as if they are part of a group - yet also want to be viewed as unique.</p> <p>Can appear to shun adult influence but still require clear boundaries and support from parents and teachers.</p>	<p>Communications with friends; games (for boys), gossip, TV/films, shopping.</p> <p>Open communication across a range of sites.</p> <p>Visual communication now vital and the 'currency' of likes and ratings is very important.</p>	<p>More settled within peer groups.</p> <p>Beginning to get better at the risk/reward equation.</p>

## References

- Carr, A. (2006) *The Handbook of Child and Adolescent Clinical Psychology: A Contextual Approach*. London: Routledge
- Deforche, B. , De Bourdeaudhuij, I, D'hondt, E, Cardon G et al. (2009) Objectively measured physical activity, physical activity related personality and body mass index in 6- to 10-yr-old children: A cross-sectional study. *The International Journal of Behavioral Nutrition and Physical Activity*, Vol 6, 6-25
- Greco, L. A. & Morris, T.L. (2005) Factors Influencing the Link Between Social Anxiety and Peer Acceptance: Contributions of Social Skills and Close Friendships During Middle Childhood. *Behavior Therapy*, 36(2), 197-205.
- Hagell, A. (ed.)(2012) *Changing adolescence : social trends and mental health*. Bristol: The Policy Press
- Hofferth, Sandra L. (2009) Media use vs. work and play in middle childhood. *Social Indicators Research*, 93(1), 127-129.
- Jellesma, F.C. & Vingerhoets A. (2012) Crying in middle childhood: A report on gender differences. *Sex Roles* 67(7-8), 412-421.
- Kern, M., Della Porta, S.S. & Friedman, H (2014) Lifelong pathways to longevity: Personality, relationships, flourishing, and health. *Journal of Personality*, 82(6), 472-484.
- Klapwijk, E., Goddings, A., Blakemore, S (2013) Increased functional connectivity with puberty in the mentalising network involved in social emotion processing. *Hormones and Behavior*, 64(2), 314-322.
- Knoll, L.J., Magis-Weinberg, L., Speekenbrink, M & Blakemore, S (2015) Social influence on risk perception during adolescence. *Psychological Science*, 26(5), 583-592.

- Martin, Cn, Dinella, L. M., (2012) Congruence between gender stereotypes and activity preference in self-identified tomboys and non-tomboys. *Archives of Sexual Behavior*, 41(3), 599-610.
- Meggitt, C. (2006) *Child Development: An Illustrated Guide*. Oxford: Heinemann
- Mills K.L., Goddings, A., Clasen, L., Giedd, J.N. & Blakemore, S (2014) The developmental mismatch in structural brain maturation during adolescence. *Developmental Neuroscience*, 36(3-4),147-160.
- Morgan, N. (2013) *Blame my brain: the amazing teenage brain revealed*. London: Walker
- Music, G. (2010) *Nurturing Natures: Attachment and Children's Emotional, Sociocultural and Brain Development*. Hove: The Psychology Press
- Sheridan, M.D., Cockerill, H & Sharma A (2007) *From Birth to Five Years: Children's Developmental Progress*. Routledge
- Smith, E. & Lillard, A. (2012) Play on: Retrospective reports of the persistence of pretend play into middle childhood. *Journal of Cognition and Development*, 13(4), 524-549.
- Vituli , H. (2009) The development of understanding of basic emotions from middle childhood to adolescence. *Studia Psychologica*, 51(1), 3-20.
- Xiaojun, Sun et al. (2009) Loneliness in middle childhood and its relation to multi-level peer experience. *Psychological Science*, 32(3), 567-570.



## 3. Evidence Section

### Risks Research: Social Media and Interactive Services

The research summary included under each of the Principles in the guide has been collated by the UKCCIS Evidence Group, a body which includes representatives from academia, government, NGOs and industry.

You can find a more detailed overview on its website at <http://www.saferinternet.org.uk/research>.

The references used for this research are the following:

#### References

- Barnardo's (2015) *Digital dangers: The impact of technology on the sexual abuse and exploitation of children and young people*. Barnardo's and Marie Curie Foundation, 2015
- Jonsson, L, Cooper, K, Quayle, E, Goran, C Svedin and Hervy, K (2015) *Young people who produce and send nude images: Context, motivation and consequences*. SPIRTO, July 2015
- Livingstone, S., Haddon, L., Vincent, J., Mascheroni, G. and Ólafsson, K. (2014). *Net Children Go Mobile: The UK Report*. London: London School of Economics and Political Science.
- Livingstone, Sonia, Kirwil, Lucyna, Ponte, Cristina and Staksrud, Elisabeth (2013) *In their own words: what bothers children online? with the EU Kids Online Network*. EU Kids Online, London School of Economics & Political Science, London, UK
- Livingstone, Sonia, Marsh, Jackie, Plowman, Lydia, Ottovordemgentschenfelde, Svenja and Fletcher-Watson, Ben (2014) *Young children (0-8) and digital technology: a qualitative exploratory study - national report - UK*. Joint Research Centre, European Commission, Luxembourg
- Livingstone, Sonia, Mascheroni, Giovanna, Ólafsson, Kjartan and Haddon, Leslie (2014) *Children's online risks and opportunities: comparative findings from EU Kids Online and Net Children Go Mobile*. EU Kids Online, LSE, London, UK
- Mitchell, Kimberly J., Finkelhor, David, Wolak, Janis, Ybarra, Michele L. and Turner, Heather (2011) *Youth Internet Victimization in a Broader Victimization Context*. *Internet Journal of Adolescent Health* 48 (2011) 128–134
- NSPCC (2015) NetAware statistics. Unpublished data.
- Ofcom (2014) *Children's media use and attitudes report*. Ofcom, London, UK
- Ofcom (2015) *Children's media use and attitudes report*. Ofcom, London, UK
- Ofcom/ESRO (2015) *Children's Media Lives – Year 1 Findings*. Ofcom, London, UK
- Ofcom/Jigsaw (2012) *Parents' views on parental controls: findings of qualitative research*. Ofcom, London, UK
- Ofcom/Sherbert (2014) *Children's online behaviour: issues of risk and trust*. Ofcom, London, UK
- Smahel, David and Wright, Michelle F. (2014) *The meaning of online problematic situations for children: results of qualitative cross-cultural investigation in nine European countries*. EU Kids Online, London School of Economics and Political Science, London, UK
- UKCCIS (2014) *Research Highlight 74: BBC survey for Safer Internet Day 2014*
- UKCCIS (2015) *Research Highlight 73: Childwise Report: Trends in media use*
- Wespieser, K. (2015). *Young people and e-safety: The results of the 2015 London Grid for Learning e-safety survey*. Slough: NFER.
- Whittle, H. C., Hamilton-Giachritsis, C. E. and Beech, A. R., 2015. *A comparison of victim and offender perspectives of grooming and sexual abuse*. *Deviant Behavior*, 36 (7), pp. 539-564.

## 4. Examples of Tools Used by Social Media Service Providers

Below are some examples of tools that can be used by social media service providers in their day-to-day operations:

- Some social media platforms can run **real name detection algorithms** to ensure that users use their real names.
  - » *This check combined with a specific number of other data checks can be used to assess the probability that the same user is setting up a new account or accessing a previously set up account.*
- Social media platforms can use **facial recognition tools** for a variety of purposes, including photo tagging, and social authentication.
  - » Facial recognition tools could be used to check for matches between a user's photos, in the deactivated profile, with those in a new profile.
- **Social graph analysis** underpins the recommendation feature 'Friends you may know.'
  - » The algorithms used to analyse social graphs could be adapted to detect the percentage of matched connections between the social graph of a de-activated account and a new profile.
- **Device fingerprinting** can be used to identify devices that click on ads and gathers non-personal data, such as the operating system version, time and other data points.
  - » *The fingerprints of the devices used to access the deactivated account can be cross-checked with those used to access a new account.*
- Cross checking the **device fingerprints, geo-location data points** and **log files of patterns of activity** associated with both deactivated and new profiles.

## 5. Contacts and Links for More Information

### Additional Resources and Contacts:

#### Resources

EU Kids Online Research - <http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx>

Ofcom's Media Literacy Research - <http://stakeholders.ofcom.org.uk/market-data-research/media-literacy>

The OFT Principles for online and app-based games - [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/288360/oft1519.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/288360/oft1519.pdf)

GSMA Privacy Design Guidelines for Mobile Application Development - <http://www.gsma.com/publicpolicy/privacy-design-guidelines-for-mobile-application-development>

and illustrative examples - <http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/usecaseannexprivacy1.pdf>

GSMA and MSRI report on Children's use of mobile phones - [http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/GSMA\\_Childrens\\_use\\_of\\_mobile\\_phones\\_2014.pdf](http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/GSMA_Childrens_use_of_mobile_phones_2014.pdf)

The public standard for age verification by the British Standards Institute (PAS 1296 Age Checking code of practice) - [www.agecheckstandard.com](http://www.agecheckstandard.com)

#### Online resources for information on abuse/misuse

MindEd is a free educational resource on children and young people's mental health for adults - <https://www.minded.org.uk/index.php>

Beat, the eating disorders charity, has published Media Guidelines for Reporting Eating Disorders - [http://www.b-eat.co.uk/assets/000/000/072/BeatMediaGuidelines\\_original.pdf](http://www.b-eat.co.uk/assets/000/000/072/BeatMediaGuidelines_original.pdf)

Digital harm and other forms of self-harassment: Report on [Digital Self-Harm](#) by Elizabeth Englander, and further information on [Digital Self-Harm and Other Acts of Self-Harassment](#)

#### Contacts

##### Child safety organisations

**Childnet International** - [www.childnet.com](http://www.childnet.com)

**CHIS** - [www.chis.org.uk](http://www.chis.org.uk)

**NSPCC** - [www.nspcc.org.uk](http://www.nspcc.org.uk)

**FOSI** - [www.fosi.org](http://www.fosi.org)

**SWGFL** - [www.swgfl.org.uk](http://www.swgfl.org.uk)

**ParentZone** - [www.theparentzone.co.uk](http://www.theparentzone.co.uk)

Contact: [info@parentzone.org.uk](mailto:info@parentzone.org.uk)

##### Law enforcement

**NCA-CEOP (National Crime Agency - Child Exploitation and Online Protection Command)** - [partnerships@nca-ceop.gsi.gov.uk](mailto:partnerships@nca-ceop.gsi.gov.uk)

**IWF (The UK Hotline for reporting criminal online content)** - [www.iwf.org.uk](http://www.iwf.org.uk)

Contact: [members@iwf.org.uk](mailto:members@iwf.org.uk)

## Authorities

**BBFC (British Board of Film Classification)** - <http://www.bbfc.co.uk/>  
Contact: [feedback@bbfc.co.uk](mailto:feedback@bbfc.co.uk)

**ICO (The Information Commissioner's Office)** - <http://www.ico.org.uk>

**ASA (Advertising Standards Authority)** - [www.asa.org.uk](http://www.asa.org.uk)  
Contact: [enquiries@asa.org.uk](mailto:enquiries@asa.org.uk)

**CAP (Committee of Advertising Practice)** - [www.cap.org.uk](http://www.cap.org.uk)  
Contact: [enquiries@asa.org.uk](mailto:enquiries@asa.org.uk)

**Ofcom (Office of Communications)** - [www.ofcom.org.uk](http://www.ofcom.org.uk)

## Industry organisations

**The ICT Coalition Principles** - <http://www.ictcoalition.eu/>  
Online form to become a member: <http://www.ictcoalition.eu/contact>

## Consultant

**Julian Coles** [julian@juliancoles.com](mailto:julian@juliancoles.com).

