Department
for Culture
Media & Sport

See more information about this Guidance

Guidance

Child Safety Online: A Practical Guide for Providers of Social Media and Interactive Services

Published 1 March 2016

Contents

↕Contents

0.1 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.

0.2 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.

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.

0.3 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.

0.4 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.

0.5 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.

0.6 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.

0.7 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.

0.8 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.

1. Section 1: About this guide

1.1 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.

1.2 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.

1.3 Defining and Differentiating 'Online Risks'

Online risk 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.
- 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, 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.

1.4 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

- 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.

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

2.1 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.

2.2 How many children are seeing negative types of content

online?

Just over one in ten (12%) of online 9-16s say they have seen sexual images online. 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. 4% said they'd seen websites where people discuss ways of committing suicide, and the same proportion (4%) said they had received "sexting" messages 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:

- approximately three children have seen online sexual images
- five children have encountered sites about physical harm
- and one child has received sexting messages (Livingstone, Haddon et al, 2014)

2.3 What do parents think of social media sites?

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:

- parents saw sexual content in 72% of the sites
- bullying in 52% of sites
- and violent/hatred content in 52% of sites. (NSPCC, 2015)

2.4 What are parents using and doing?

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. (Ofcom, 2015)

2.5 Good Practice

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

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).

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.

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 * references to sexual violence

You can see their full criteria here.

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).

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.

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.

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.

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
- stay informed about the development of a public standard for age verification by the British Standards Institute (e.g. http://www.agecheckstandard.com).

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.

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.
- 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 • 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.

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.

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.

2.6 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.

It's 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.

What are parents using and doing? 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. (Ofcom, 2015)

Are they using technical tools? 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 (Ofcom, 2015).

Do parents know what their children are doing? 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. (Wespieser, 2015)

2.7 Good Practice

Consider parental controls that are designed for your service.

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

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:

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.

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.

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:

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.
- You can also check if your URL is restricted by an ISP in the UK at 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).

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, mobiles phones,

games consoles and internet-enabled hardware such as televisions, domestic appliances and wearables.

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.

2.8 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. . 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.

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
- 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.

What types of online contact are important to children? 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. Particularly for girls, image is critical. For boys, appearing funny and laidback is more important. (Ofcom/Sherbert, 2014)

What types of contact are they having online? 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. 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. (Ofcom, 2015)

Have they experienced negative contact online? When asked directly: * 4% of all 12-15s and 1% of all 8-11s say they were bullied on social media in the last year. * 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. (Wespieser, 2015)

2.9 Good Practice

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).

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.
- 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

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.

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.
- 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).

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.
- 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.

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
- As well as giving general information about staying safe on their platform, companies often work with local experts to provide specialist resources

2.10 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.

2.11 Good Practice

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

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

- IWF: 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

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.
- 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)

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'.

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 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 for more information or contact 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 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

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:

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:

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.

2.12 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.

How many children are seeing negative types of content online?

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 (Livingstone, Haddon et al, 2014).

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". (Smahel and Wright, 2014)

What techniques do they know about and use – to avoid or court risks?

Among online 12-15s: * 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 * 15% say they have changed their social media settings to be more private, and 35% say they know how to do this * 7% say they have reported something online that they found upsetting, with 29% knowing how to do this

On the other hand: * 11% say they have deleted history records (34% know how to) * 6% have amended privacy settings (24% know how to) * 1% have unset filters or controls (10% know how to) (Ofcom, 2015)

2.13 Good Practice

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.

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'.

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.

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.

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.

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

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

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

2.14 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.

What do parents know? 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. (Ofcom, 2015)

What do children want? 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. (Smahel and Wright, 2014)

Do children understand what they're being told? 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. (Ofcom/ESRO, 2015)

2.15 Good Practice

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.

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 AntiBullying 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.

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 selfharassing/bullying), suicide and general online safety issues.

2.16 Examples of Organisations

The UK Safer Internet Centre 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.

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.

2.17 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 and UKIE to help promote online child safety issues more generally.

2.18 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]9http://www.microsoft.com/about/corporatecitizenship/en-us/youthspark/youthsparkhub/programs/onlinesafety/resources/), 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

3. 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.

3.1 A note on moderation

In this guide, ‘pre-moderation’ refers to content reviewed by a service provider before it becomes visible to others. ‘Postmoderation’ 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.

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.

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.

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.

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.

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 and the ASA.

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.

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.

Inappropriate behaviour needs warnings in clear and understandable language.

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

Actively manage your community, complementing the areas that premoderation alone can't address.

Try to make your responses constructive and positive.

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.

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.

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

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.

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.

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.

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.

Services and information

Benefits

Births, deaths, marriages and care

Business and self-employed

Childcare and parenting

Citizenship and living in the UK

Crime, justice and the law

Disabled people

Driving and transport

Education and learning

Employing people

Environment and countryside

Housing and local services

Money and tax

Passports, travel and living abroad

Visas and immigration

Working, jobs and pensions

Departments and policy

How government works

Departments

Worldwide

Policies

Publications

Announcements