



Market Data / Supplier Selection /  
Event Presentations / **Best Practice** /  
Template Files / Trends & Innovation



# Child Protection Online

Best Practice Guide

# Child Protection Online

## Best Practice Guide



**Published July 2009**

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording or any information storage and retrieval system, without prior permission in writing from the publisher.

Copyright © Econsultancy.com Ltd 2009

**Econsultancy London**  
4th Floor, 91-93 Farringdon Rd  
London EC1M 3LN  
United Kingdom

Telephone:  
+44 (0) 20 7269 1450

<http://econsultancy.com>  
[help@econsultancy.com](mailto:help@econsultancy.com)

**Econsultancy New York**  
41 East 11th St., 11th Floor  
New York, NY 10003  
United States

Telephone:  
+1 212 699 3626

# Contents

1. Introduction.....	1
2. Law: Interpretation and Approach.....	2
2.1. Introduction.....	2
2.2. UK Laws.....	2
2.2.1. UK's Data Protection Act 1998.....	2
2.2.2. Sexual Offences Act 2003.....	2
2.3. Untested Laws to Be Cautious Of.....	3
2.4. EU Directives and Best Practice.....	3
3. Setting Up a Safer Community.....	4
3.1. Risk Assessment.....	4
3.2. Moderation.....	5
4. Technology.....	6
4.1. Top Tools to Maximise Effectiveness.....	6
4.2. Advanced Moderation Technologies.....	6
4.3. Privacy Enhancing Technologies.....	7
5. Recruitment and Training.....	8
5.1. Recruitment.....	8
5.1.1. Recruitment Adverts.....	8
5.1.2. References.....	8
5.1.3. Interviews.....	9
5.1.4. Contracts / Terms of Employment.....	9
5.2. Training.....	9
5.3. Staff Protection.....	10
6. Escalation Procedures.....	11
6.1. Reporting Mechanisms for Users.....	11
6.2. Internal Escalation.....	12
6.3. External Escalation.....	12
7. Marketing To Young People via Communities.....	14
7.1. Key Issues.....	14
7.2. Collecting Online Data: What You Need to Know.....	15
7.3. Before Launching Any Social Media Project for Children.....	15



8. Safety & Education.....	16
9. Terms of Service.....	17
9.1. Education.....	17
9.1.1. Teachtoday.....	17
9.1.2. CEOP.....	18
9.1.3. Childnet International.....	18
9.1.4. ChildLine.....	18
9.1.5. DCFS.....	18
9.1.6. Tips on keeping safe on social networking services.....	18
10. Summary.....	19
11. About Tempero.....	20
11.1. About the contributors.....	20
12. About Econsultancy.....	21



# 1. Introduction

**Child safety should always, without doubt, be the number one priority for those managing Social media projects.**

The explosion in user-generated content (UGC) and social media in recent years has meant young people are now spending the majority of their spare time online and brands and marketing agencies are building their own, or joining existing, online spaces to exploit the ever growing audience.

The Government has taken children safety online seriously with the setting up of the Internet Task Force on Child Protection in 2000 and recently set up the UK Council for Child Internet Safety following an independent review commissioned by the Prime Minister.

The review recognised the need for law enforcement, children's charities and the whole range of industry players involved in providing online services in the new digital age, including marketers and advertisers, to provide better safeguards to protect children online.

Despite the huge range of benefits to be gained from social media, navigating the complex web of process, procedures, guidance and law can be time consuming, confusing and ultimately damaging if followed incorrectly.

This guide aims to introduce and make recommendations specifically for brand owners or agencies thinking about building or joining an online community.

## 2. Law: Interpretation and Approach

### 2.1. Introduction

While in the US there is specific legislation directed at the protection of young people online in the form of the Child Online Privacy Protection Act ("COPPA") there is no equivalent at present in UK law which specifically addresses children and young people. The UK Data Protection Act 1998 makes no distinction based upon age. This environment is largely viewed as being self-regulated.

The obligations of community owners will be changed unrecognisably if OFCOM or an equivalent UK governmental organisation is given the remit of regulating the online environment.

There have been a number of recent indications from the Department for Culture Media and Sport that it believes that formalised regulation is both necessary and inevitable and there is even talk of a Communications Act 2009 which will impose regulation on the web, however it is very much a case of "watch this space" for now.

In the meantime there are some existing laws and EU directives which provide guidance in this area.

### 2.2. UK Laws

In the UK, many of the existing laws are increasingly being used to fill the gap.

#### 2.2.1. UK's Data Protection Act 1998

This is one of the key areas to be aware of in the UK. It does not specifically refer to the protection of data relating to young people, but the Information Commissioner's Office (which is responsible for implementing UK Data Protection legislation) has indicated that:

*"Websites that collect information from children must have stronger safeguards in place to make sure any processing is fair. . . The language of the explanation should be clear and appropriate to the age group the website is aimed at.*

*"If you ask a child to provide personal information you need consent from a parent or guardian, unless it is reasonable to believe the child clearly understands what is involved and they are capable of making an informed decision."*

#### 2.2.2. Sexual Offences Act 2003

Clearly one of the key concerns in relation to the involvement of young people in online communities is the issue of grooming. The provisions of the Sexual Offences Act 2003 can be used to prosecute individuals who use online environments for grooming.

Under the Act it is an offence for anybody over 18 to befriend a person younger than 16 and then meet or intend to meet that young person anywhere in the world with the intention of sexually abusing them. The Act carries a maximum sentence of 10 years.

The UK also has a specific police body, the Child Exploitation and Online Protection Centre (CEOP) which works in conjunction with local police forces and other police forces around the world to tackle the sexual abuse of children and to enforce the provisions of the Sexual Offences Act. It is a body to which both children and parents can report any concerns they have regarding the behaviour of users online.

## 2.3. Untested Laws to Be Cautious Of

There are still a number of web related issues that have not been tested in the UK courts as both the courts and the regulators are trying to catch up with a raft of emerging privacy, defamation, data protection and IP issues that can arise in the online environment.

As more and more issues arise and more cases get to court the law in this area is slowly developing. With such a new industry it is important to watch out for prominent cases and landmark rulings which will clarify the grey areas. However, remember that outcomes in overseas courts provide guidance only as they might not be repeated in UK courts.

The UK courts are yet to consider the question of whether a web site operator should be held responsible for the publication of unlawful content featured on a third party site where the web site user in question has directed users of its own site to that content by way of links.

Similarly the question of whether or not a user of a social networking site waives their right to privacy under Article 8 of the European Convention on Human Rights by publishing private information on their profile online has yet to be debated by the UK courts. An indication of the US answer to this question occurred recently.

The Californian Court of Appeal recently held that no reasonable person would have an expectation of privacy regarding information that he or she has freely disseminated on a public social networking Web site. (*Moreno v. Hanford Sentinel Inc.*, No. FO54138 (Cal. Ct. App. Apr. 2, 2009)).

The site on which the information was uploaded in the particular case was MySpace, where information is made available to anyone accessing the site. However, it is very possible that the court may decide differently in the case of sites such as Facebook or Flickr where access to information uploaded by users can be expressly limited to a small group of nominated friends. Again, remember US cases aren't binding in the UK so this decision is of useful guidance only.

## 2.4. EU Directives and Best Practice

Industry dialogue has taken place across the EU and best practice guidelines established (Safer Social Networking Principles for the EU). The benefits for brands now managing or interacting in online communities are twofold, protecting young people and also upholding their reputations as responsible corporates.

### 3. Setting Up a Safer Community

Deciding what safeguards are necessary for a web service or community is not prescriptive. Safety needs vary based on level of interaction or UGC allowed and age of young people using community.

For example those aged almost 18 years old are more capable of understanding risk and making informed decisions compared too much younger children.

The Byron review recognised the potential risks to children as set out in this table (Developed by the EUKids Online project – Hasenbrink ,Livingstone, Haddon, Kirwi and ponts,2007):

	<b>Commercial</b>	<b>Aggressive</b>	<b>Sexual</b>	<b>Values</b>
Content (child as recipient)	Adverts Spam Sponsorship Personal Info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info
Contact ( child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers  Being groomed	Self-harm  Unwelcome persuasions
Conduct(child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/advice

#### 3.1. Risk Assessment

In general risk assessment considers areas such as:

- Is the service or interaction specifically targeting children and younger users?
- What is the likelihood of the service attracting children or young users due to its theme *e.g.* football or celebrities?
- If contact and interaction with strangers is enabled.
- Is anonymous or non-verified user registration possible?

A rigorous 10 point checklist which is particularly useful to those creating an interactive community is available to download from the Home Office.



## 3.2. Moderation

The Home Office Good Practice Guidance for the providers of Chat Services, Instant Messaging and Web Based Services supports moderation in services for children and young people.

Having undertaken a risk assessment, it is necessary to decide which form of moderation or combination of forms is appropriate.

Types of moderation:

Type:	What is it?	Pros:	Cons:
<b>Technical Moderation:</b>	Software filters words, phrases, telephone and email address formats, profanities and explicit language	Automated Cost effective Range of choice Can prioritise content/issues	Users can get around May frustrate users with legitimate requirements Minimal user protection Minimal brand/reputation management
<b>Human moderation:</b>	Volunteers or trained professionals who can understand social nuances and judge appropriate content and behaviour	More effective minimising risk Better brand management	Can be labour intensive More expensive than automation
<b>Pre-moderation:</b>	Content is pre-approved before it's published	Best for minimising risk Suitable for young people or at risk communities	Even a short delay can frustrate users Labour intensive on high traffic sites
<b>Post-moderation:</b>	Content reviewed after it's published	Ensures conversations can take place in real-time, but still remain protected	Moderate risk inappropriate content/behaviour may appear on site
<b>Reactive moderation:</b>	Content reviewed only in response to being "flagged" as inappropriate	Good for high traffic, lower risk site	Inappropriate content/behaviour will remain on site until reported Relies on users to self-police

## 4. Technology

When it comes to moderating children's social media, the more protection in place, the better and intelligent technologies are starting to become a useful tool in the armoury. Traditionally, moderators have only had the aid of profanity and keyword filters but 2009 is going to be the year when more advanced moderation tools come of age.

The cheaper automated tools will look attractive to those on a tight budget but the health warning with that is no technology is failsafe and when it comes to child safety in particular, an understanding of the human condition is paramount. One of the best ways to consider any automation is as a tool for prioritisation of dealing with content rather than pure automation.

The critical advantage of the higher specified artificial intelligence type tools is the ability to track long term behaviours and patterns. Add this to the more subtle eye of a trained moderator and you have the best combination of protection currently available.

### 4.1. Top Tools to Maximise Effectiveness

Providing safe environments online requires a combination of approaches for maximum effectiveness. Here are the three key areas where technology can help:

- **Robust registration:** Pre-moderate profiles, enforce users to provide valid email addresses and tick they've read the house rules (and ideally safety notices)
- **Moderation system:** However the content is to be moderated, a professional, efficient moderation system will help to minimise issues (if used correctly)
- **Report abuse / inappropriate content:** Users need clear and simple ways of alerting inappropriate activity to moderators and site administrators.

### 4.2. Advanced Moderation Technologies

#### [NetModerator](#)

This is designed to detect grooming patterns and behaviour; the application can be applied to many forms of content and applies learning technology to continually improve the process.

#### [Keibi](#)

This is a US based company with some advanced image recognition tech - great for helping to filter inappropriate images from profiles and UGC areas.

#### [Con-Trust](#)

Comprehensive text, image and video moderation software which can be used with a variety of platforms.

## 4.3. Privacy Enhancing Technologies

If adding a community into operations you may now become responsible for holding and protecting data of non-employees. It's advisable to ensure compliance with the Data Protection Act 1998 and evaluate if your business technology needs reviewing e.g. access to data by employees, security permissions, robust firewalls etc.

- The Information Commissioners Office [outlines your legal obligations](#).
- There is also a [useful guide](#) to audit your systems and processes.

**Please note Third Party suppliers who have access to or are responsible for holding data will need to be compliant.**

# 5. Recruitment and Training

Recruitment and training are crucial parts of the protection process in setting up and managing community and moderation services.

Recruiting a moderator working on areas which may attract children should be managed in the same regulated way you would recruit for teacher or other professions which may involve working with children.

## 5.1. Recruitment

### Independent Safeguarding Authority (ISA)

The Independent Safeguarding Authority (ISA), is the new vetting and barring scheme and will have a major impact on the recruitment and monitoring practices of people working or volunteering with children.

Created under the Safeguarding Vulnerable Groups Act 2006, the new vetting and barring scheme will replace the current List 99, PoCA and Disqualification Orders regimes. The ISA will decide who is unsuitable to work or volunteer with vulnerable groups. It will base its decisions on pulling together information held by various agencies, government departments and the Criminal Records Bureau (CRB).

There are two forms of CRB checks – standard and enhanced (for more information about the different types of checks you can go to <http://www.crb.gov.uk/>). Enhanced checks are recommended for moderators working on areas which are likely to attract children.

Once the scheme is fully rolled out, it will be illegal to hire someone in regulated activity who is not registered, and has therefore not been checked by, the ISA. The new scheme will cover employees and volunteers in the education, care and health industries, affecting some 11.3 million people.

The new law will be phased in by 12 October 2009 to control organisations that provide moderated services aimed at children and vulnerable adults. The new law will prohibit anyone *'moderating a public interactive communication service which is likely to be used wholly or mainly by children'* who is registered on the list of banned people.

### 5.1.1. Recruitment Adverts

Advertisements should be clearly defined and placed within the relevant trade publications and organisations.

Within the advert it should clearly state that all successful employment will be subject to a Disclosure via the Criminal Records Bureau and additional background checks, establishing their suitability to work with children.

### 5.1.2. References

Written references from current and previous employers should be supplied. Reference requests should include key information about the job application and should comment on character, performance, strength and weaknesses.

Candidates should supply full employment history, including any periods of unemployment with exact dates

### 5.1.3. Interviews

Interviews should be face-to-face, ideally with a minimum of two members of senior management.

**Interviews should include:**

- Positive identification checks (in line with money laundering legislation).
- Discussion of the position.
- Aptitude tests covering moderation judgement, technology, grammar, and attention to detail.
- General interview to test for understanding of the interactive moderation industry and suitability for working within a moderation environment.
- Value-based questions designed to test the candidate's suitability for working with children (these should be constructed with a childcare recruitment expert).

### 5.1.4. Contracts / Terms of Employment

**These should include:**

- Confidentiality and data protection clauses.
- Declaration of all convictions included those regarded as “spent” (as employment should be subject to exemption from the provisions of the Rehabilitation of Offenders Act 1974).
- Provision to enable termination if employee has failed to disclose any such conviction.
- Suitable probationary periods (measured on performance and suitability for continued employment).
- Internal policy preventing employees contacting children / users outside of their working requirements.
- Prevention of use of moderation screen name outside of working hours.

## 5.2. Training

The training of moderators needs to cover a number of key areas so they have an awareness of relevant issues and policies and can operate effectively. It is not critical whether training is provided in-house or by use of outside expertise.

What is important is that the training prepares the moderator to apply their knowledge effectively. The training should reflect the realities of what is possible for the moderator in the particular environment.

**Based on your risk assessment some or all of the following may be relevant:**

- Understanding the role of a moderator.
- Site moderation guidelines and editorial policies.
- Understanding and identifying concerning / inappropriate user behaviours.
- Comprehensive training on child protection and recognising potential grooming behaviours.
- Identifying and preventing potential bullying/harassment.
- Comprehensive legal training - recognising and preventing illegal or harmful content.
- Data protection and security training.

- Internal and external escalation procedures.
- Interacting with users / brand representation (if required).

For further guidance please also reference Home Office '[Good practice guidance for the moderation of interactive services for children](#)' and also Home Office Task Force on Child Protection on the Internet: [Good practice guidance on Chat, Instant Messaging, Web Based Services, Moderation, Safe Search and Social Networking Services](#).

## 5.3. Staff Protection

When employing moderators it is essential that stringent management policies are implemented to ensure your staff are protected within their working practice.

### **Some of the areas which should be considered include:**

#### **Protecting user data**

Systems and moderator accounts should be restricted to ensure moderators only have access to user personal data in order to enable them to provide the moderation services.

If your service only requires moderators to moderate within the public areas, user data such as email addresses and other personal information should therefore be restricted on moderator accounts.

#### **Storing moderation actions**

Moderation applications and technology should be developed to ensure all moderator actions can be fully stored and archived.

Where possible moderators should also work using individual moderator ID's so all activities can be fully recorded and accountable during their moderation shifts.

#### **Exposure to highly inappropriate / harmful content**

In line with escalation procedures and policies, moderators should be trained in managing and escalating potentially illegal / concerning content. Procedures should ensure that inappropriate / illegal content is isolated and other members of staff are not exposed to the content.

Support / counselling services should also be offered to moderators where possible, to allow for moderators to discuss concerns and emotional issues regarding exposure to concerning content of this nature

#### **Management and Supervision**

Managers should supervise and support moderators during all service hours. If moderators are working remotely from the office, supervision procedures should include additional measures to ensure moderators are fully accountable at all times and work stations are protected to ensure content and user data is secure.

## 6. Escalation Procedures

The internet has recently experienced a significant step forward in its evolution with the emergence of user interactive services, headed by social networking services and video sharing websites.

However with all emerging technologies there is also the potential for misuse. Most online communities have set boundaries on the use of their service, including what is acceptable and unacceptable behaviour, and provide robust procedures for handling complaints including a range of concerns which may potentially arise in online communities.

During the course of managing a brand or marketing campaign on an interactive service you may come across content which concerns you.

It is therefore important that marketing professionals are aware of the terms of service, including acceptable behaviour and are aware of the procedures for handling complaints and also have internal procedures in place to escalate concerns the appropriate authorities.

### 6.1. Reporting Mechanisms for Users

Home Office guidance emphasises the need for users to be able to access straightforward mechanisms to report concerns, including:

- Posting images depicting child sexual abuse or exploitation.
- Suspicious behaviour towards children and young people, including behaviour indicative of grooming.
- Bullying and harassment.
- Posting of inappropriate content, such as information promoting or encouraging self-harm, suicide or eating disorders.
- Incorrectly tagged adult or age – inappropriate content and other potentially illegal or criminal behaviour.

Within communities where users violate the terms of service, incidents may fall into the minor which can be dealt with internally, up to the serious which, in some cases, may even constitute a crime.

While in the offline world crime reporting is fairly straight forward, investigating crimes committed in online environments is still a relatively new concept for law enforcement.

However, Home Office good practice guidance for the providers of social networking recognises the great deal of work which has been achieved in combating illegal activities online:

*“Service providers and law enforcement agencies have achieved a great deal of success in cooperating effectively to combat illegal activities online using well-established protocols and procedures.”*

## 6.2. Internal Escalation

Those managing interactive communities should have an internal escalation procedure to ensure consistency of response to concerns reported by users. Internal escalation should begin with a concern being raised for a second view and a risk assessment about action required to be taken.

### **This will require an assessment based upon:**

- The information presented.
- The context in which the concern has arisen i.e. an interactive service aimed at children.
- The nature of the concern i.e. a child or young person posting a message saying that they are going to kill themselves or a child asking for advice because their parents are divorcing.
- The risk to life, whether it is an emergency.
- If it is potentially illegal.

It's up to individual companies to decide themselves the best internal escalation process.

### **Consider one or all of the below:**

- Referring young people to official advice on general health and relationship issues or to children's welfare organisations who offer confidential help and support.
- If it is potentially illegal content or activity report to the police.
- If it is an emergency situation i.e. an immediate risk or threat to life, it should be escalated and reported immediately to the police on 999.

## 6.3. External Escalation

### **The Home Office Guidance contains recommendations on:**

- Reporting mechanisms for users to report suspected child abuse.
- Placing advice, information and links where users are interacting with other users.
- A general page with information and/or links.

### **Organisations for external escalation include:**

- The service provider.
- Law enforcement agencies.
- Emergency services where there is an immediate threat to safety of life, or where a child or children are at immediate risk of harm – call the police on 999.
- Child welfare agencies such as ChildLine/NSPCC.
- Child Exploitation and Online Protection Centre.
- The Internet Watch Foundation. This is the UK internet hotline for reporting illegal online content, specifically child sexual abuse images hosted worldwide and criminally obscene and incitement to racial hatred content which is hosted in the UK.

## Directory of agencies for external escalation issues:

Escalation issues:	Related Agencies
Cyberbullying	<a href="#">Department for Children and Family Services (DCSF)</a> <a href="http://www.police.uk/forces">Police ( www.police.uk/forces)</a> <a href="#">Kidscape</a> <a href="#">NSPCC</a> and <a href="#">ChildLine</a>
Exploitation, abduction and trafficking	<a href="#">NSPCC</a> and <a href="#">ChildLine</a> <a href="#">CEOP</a> <a href="#">United Kingdom Human Trafficking Centre</a>
Health related issues	<a href="#">ChildLine</a> <a href="#">Connexions</a> <a href="#">Harmless</a> <a href="#">Mental Health Foundation</a> <a href="#">National Self-Harm Network</a> <a href="#">Samaritans</a> <a href="#">The Site</a>
Discrimination or hatred based on race, gender or sexuality	<a href="#">CrimeStoppers</a> <a href="#">London Lesbian and Gay Switchboard</a> <a href="#">NSPCC</a> and <a href="#">ChildLine</a> <a href="#">Victim Support</a>
Physical or verbal abuse including sexual abuse	<a href="#">NSPCC</a> and <a href="#">ChildLine</a> <a href="#">Women's Aid</a> <a href="#">CrimeStoppers</a>
Terrorism and bomb threats	<a href="#">Police Anti-Terrorist Hotline</a>

# 7. Marketing To Young People via Communities

The [Safer Children in a Digital World Report](#) resulting from the [Byron Review](#) in 2008 outlined that advertisers have the potential to play an important role in driving standards for responsible online content.

Clear conduct has already been set out by the Committee of Advertising Practice ([CAP](#)) Code which is administered by the Advertising Standards Authority ([ASA](#)) and the review praised the industry for being proactive in putting in a self-regulatory system to minimise the exposure of children to inappropriate products and advert content.

However, in 2006 the ASA was unable to investigate 90% of the 2,000+ complaints it received relating to online advertising as they were outside its remit. This illustrates that a new medium and evolving advertising has created some online specific safety issues.

## 7.1. Key Issues

- **Advertising alongside inappropriate content:** Concern that well-known brands appearing alongside may legitimise that content in the eyes of a child.
- **Ad wise:** Children and young people are unlikely to understand the complexities of online advertising e.g. interactive games.
- **Age verification:** establishing age with regards to accessing content is difficult online. The traditional broadcast advertising “watershed” doesn’t assist in naturally filtering younger users online.
- **Nurturing online discussions:** appropriate online campaigns around sensitive subjects, for example harmful behaviours, if interactive could then evolve into negative conversations.
- **Offline events:** Online activity facilitating offline interaction where young people may be more at risk of meeting strangers.
- **Privacy and collection of personal data:** By far the biggest issue in the online space and made even more problematic by the proliferation of unregulated online competitions for the purposes of data capture.

## 7.2. Collecting Online Data: What You Need to Know

Guidance for this area comes from the [Data Protection Act 1998](#) and [Privacy and Electronic Communications \(EC Directive\) Regulations 2003](#).

Many brands operating communities or running campaigns within communities are arguably non-compliant by failing to make clear how they will be using information they collect, assuming that the use of the personal information is obvious.

While that may be true for registration or personal profile building, making use of or selling that data for marketing purposes requires user consent. Young people are particularly vulnerable if providing personal information and with children, age dependent, there is concern over the ability to give that consent.

Transparent data collection also extends to automatic tools such as cookies, IP identification, or other tracking and collection tools such as spiders.

A privacy statement held generically on a website is not enough. Those collecting data must show a basic description of the use of that information wherever it is collected. This information, when communicated to young people must be easy to understand and age-appropriate.

Age appropriateness can vary widely, for example within a short age gap like 10 to 12, so a community with young people from 8 to 18 would need multiple versions of this information, including a process to encourage children to involve parents in the permission process.

## 7.3. Before Launching Any Social Media Project for Children

Regulation and legality aside, applying real world common sense is vital. Stranger danger is as prevalent online as it is offline, more so in fact, and although it's very easy to get excited about providing children with myriad communication tools, stepping back and assessing the risks first is a must.

One very important reason for doing this is to ensure you have the tools in place to manage the content effectively from the outset. Retro-fitting moderation tools is a costly exercise and can be avoided if appropriate planning is carried out before launch.

This planning will help to assess the risks and may very well affect the route taken and how that route affects the marketing objectives and plans, the data being collected and the potential results and ultimately the project budget.

## 8. Safety & Education

While encouraging appropriate behaviour amongst community members themselves is the first step to minimise safety risks, it's important to mention the [Home Office Good Practice Guidance](#) for the providers of chat services, instant messaging and web-based services supports moderation in services for children and young people.

But aside of moderation and management, how do you create a proactive and responsible community as well as cover yourself? Clearly outlining Terms of Use and then making sure they're adhered to is a 'no brainer' in that respect, however managing child safety via terms becomes challenging when considering the Information Commissioners statement on the Data Protection Act with regards to web sites:

*"You should recognise that children generally have a lower level of understanding than adults, and so notices explaining...should be appropriate to their level... the language of the explanation should be clear and appropriate to the age group the website is aimed at."*

Therefore communicating to young people unacceptable behaviours, such as cyber-bullying, or the risks of sharing personal information could vary greatly between age groups and even necessitate an educational approach while informing of the site's specific stance on these behaviours.

## 9. Terms of Service

### Considerations to minimise risks to young people:

- **Age-appropriate:** If community or platform is used by or specifically aimed at young people your terms of service themselves should be clear and age appropriate.
- **Parental consent:** Under the Data Protection Act 1998 if you ask a child to provide personal information you need consent from a parent or guardian unless it is reasonable to believe the child clearly understands what is involved and they are capable of making an informed decision.
- **Risk Awareness:** Children need to be informed, and updated regularly, of the risks to themselves or others if misusing the web site or service.
- **Report Abuse:** There should be a simple process for anyone in the community to alert the service provider of content or behaviour which they feel violates the terms of service or find objectionable (site owners should have a policy and process in place to acknowledge and act on these reports within an appropriate time frame).
- **Privacy statement:** Privacy and data protection compliance needs to be outlined (For further information and recommendations please refer to our section on marketing to young people).

### 9.1. Education

Education plays a crucial role in keeping children and teens safer online and encouraging safe responsible use alongside technical filters and moderation.

It has long been recognised that tech savvy children and young people can bypass technical filters and the various safety measures put in place by service providers. Experience has also shown that internet users, including children, behave in more inappropriate and, at times, extreme ways online than they would offline.

Some children will engage in behaviour that may place them at risk, such as giving out personal information about themselves and will test out their sexual identities by engaging in cyber sex, and generally acting out behaviours they would not in real life.

There is a wealth of available resource produced by Government, industry and children's charities which can not only advise community owners on managing risk but also provide information and advice which could be incorporated into your site, from external links to embeddable videos. Resources include safety tips, awareness videos and specific resources for use in schools.

#### 9.1.1. Teachtoday

Resources particularly tailored towards educators to equip and empower children and young people with the tools, knowledge and skills to use ICT in a positive and responsible way and thereby gain the maximum benefits.

This resource has been contributed and collated here from major industry players, such as AOL, MySpace, Orange, YouTube, and Microsoft, which provides guidance and even shares examples of best practice implementation.

<http://www.teachtoday.eu>

### 9.1.2. CEOP

The Child Exploitation and Online Protection (CEOP) Centre is dedicated to eradicating the sexual abuse of children. They provide training, publications and age appropriate learning resources for young people

<http://www.ceop.gov.uk/>

CEOP's newly designed Thinkyouknow website will collate a comprehensive resource library

<http://www.thinkuknow.co.uk/sido9/portal/>

### 9.1.3. Childnet International

Childnet International, a charity that is helping to make the internet a great and safe place for children, have developed a set of award-winning resources called Know IT All. The resources aim to help educate young people, parents, teachers and volunteers about safe and positive use of the internet.

[www.childnet-int.org](http://www.childnet-int.org)

### 9.1.4. ChildLine

ChildLine is a service provided by the NSPCC offering a free and confidential helpline for children in danger and distress. Children and young people in the UK may call 0800 1111 to talk about any problem, 24 hours a day. The ChildLine service is delivered in Scotland by Children 1st on behalf of the NSPCC.

[www.childline.org.uk](http://www.childline.org.uk)

### 9.1.5. DCFS

Cyberbullying, a whole-school community issue

[www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/](http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/)

### 9.1.6. Tips on keeping safe on social networking services

Home Office Taskforce on Child Protection and the Internet: Good practice guidance for the providers of social networking and other user interactive services 2008.

Tips for children and young people and also for parents and carers.

[www.police.homeoffice.gov.uk/operational-policing](http://www.police.homeoffice.gov.uk/operational-policing)

## 10. Summary

Examining child safety online throws up a host of negatives issues; some of which exist in the offline world and others which have developed through the use of social media and UGC. It would be easy to feel perhaps we need to restrict young people from online interaction entirely or, at the least, not attempt to engage with them in community spaces.

However it's important to weigh up the risks with the benefits, as well as the realities of modern day living. The internet is an essential part of young people's daily lives, trying to restrict them totally, would be unrealistic and potentially force them into unregulated and even more unsafe environments. Likewise, it's only natural that brands will have to follow this generation into their preferred medium just as they have previously from print, to radio, then television.

When communities are managed and risks are minimised, social media is a fantastic and unrivalled environment for young people to socialise, engage, learn and develop. It's now up to all of us from agencies, to brands to public bodies, to ensure we carry out our duty of care and provide the highest level of protection available at our disposal.

# 11. About Tempero

Tempero is Europe's largest supplier of Social Media Moderation and Management in Europe, reviewing millions of messages 24/7 in 13+ languages.

Since its inception in 2003, Tempero has taken great pride in playing an active role in driving policy and communicating with key stakeholders on how to deliver best practice, without compromising the fun aspects of online socialising.

As an industry, Social Media is moving at an incredibly frenetic pace and keeping up with the issues, technology, public perception and burgeoning regulation is becoming increasingly difficult. Tempero pride themselves on providing a practical approach to Social Media and enable clients to benefit from advantages in the most cost effective and ultimately safe way possible.

Call us today to see how we can save you time, money, and stress +44 (0) 20 7636 1200 or contact us [online](#).

<http://www.tempero.co.uk>

.

## 11.1. About the contributors

### **Chris Atkinson**

Chris Atkinson is a child protection professional with over 10 yrs online children's safety experience and has worked for the NSPCC and CEOP including setting up the UK safety operations for a major social networking service. Chris was also a Board Director for the IWF. Chris recently set up the UK safety operations for a major social networking service. Chris works with Tempero providing training and consultancy on safety issues.

### **Sarah McColl**

Sarah McColl is a Solicitor Advocate at Wiggin LLP, a specialist media law firm which focuses exclusively on the film, music, sport, gaming, technology, broadcast and publishing sectors. Sarah regularly advises clients in relation to website content and other emerging issues in the digital arena.

## 12. About Econsultancy

Econsultancy is the leading source of independent advice and insight on digital marketing and e-commerce.

Our reports, events, online resources and training programmes help a community of over 80,000 registered marketers make better decisions, build business cases, find the best suppliers, look smart in meetings and accelerate their careers.

Econsultancy is an [award-winning online publisher of reports](#) covering best practice, user experience benchmarking, market data and supplier selection aimed at internet professionals that want practical advice on all aspects of ebusiness.

Econsultancy also operates a highly popular [training](#) division, used by some of the world's most prominent brands for staff education, both in-house and via public courses. We provide training across all areas of digital marketing and at all levels from one day courses to diplomas to Masters in Digital Marketing.

In addition, we host more than 100 events a year, such as The Online Marketing Masterclass, regular Supplier Showcases and Roundtables, an annual Future of Digital Marketing event, Digital Cream and a range of social events.

The [Econsultancy](#) site now attracts over 180,000 unique users per month where they access research, read the blog and take part in discussions in the forums. And as a portal to the digital marketing community, Econsultancy members can also link up with other members and digital suppliers through our directories, as well as find a new job or new digital talent using the job listings.

Some of Econsultancy's client-side members include: Google, Yahoo, MSN, MySpace, BBC, BT, Shell, Vodafone, Yell.com, Dell, Oxfam, Virgin Atlantic, TUI, Barclays, Carphone Warehouse, IPC Media, Deloitte, T-Mobile and Estée Lauder.

[Join Econsultancy](#) today to learn what's happening in digital marketing – and what works.

Call us to find out more on +44 (0)20 7269 1450 or [contact us online](#).

