Social networking services, social media and sport: Guidelines for safeguarding children and young people

Contents

Executive summary

Interactive social media technology has revolutionised the way that people connect and interact. Facebook, Twitter, blogs, instant messaging and photo and video exchange sites are increasingly popular, and provide an opportunity for the sporting world to connect with children and young people.

However the use of social networking sites also introduces a range of potential safeguarding risks to children and young people (described below). The NSPCC Child Protection in Sport Unit has been commissioned by Sport England to provide these safeguarding guidelines for County Sports Partnerships, National Governing Bodies and other sports organisations.

As sports organisations increasingly use social networking and other developing media to communicate with young people it is critical that safeguarding protocols and practices keep pace with the raft of communication methods young people use.

This guidance focuses on the use of social networking media and provides a simple safeguarding checklist to enable you to update your current safeguarding policy:

CPSU BRIEFINGS

Planning your social media strategy
Incorporating safeguards when setting up your social networking page
Promoting child safety online
Reporting safeguarding concerns
Working with the service provider

Purpose of this guidance

This briefing has been produced to provide information, advice and guidance on social networking services and other user interactive services to enable County Sports Partnerships, National Governing Bodies and other sports organisations considering or already using social networking media to:

1. recognise that this medium provides opportunities to effectively engage with a wide range of audiences, especially young people
2. understand the potential safeguarding risks of using social media
3. provide good practice guidelines for the safe use of social media:
    - find out more about the safety tools provided by social networking service providers and their acceptable use policies
    - take the appropriate steps to safeguard the sport's profile and its supporters online, in particular children and young people
    - promote safe and responsible use by supporters of a sports organisation
    - assist those organisations with an existing presence on user interactive services to develop, review or update their policies and practice guidance.

This guidance reflects the good practice guidance produced by the Home Office Task Force on Child Protection[1] on the Internet, with particular reference to the sporting environment. It is recognised that 'technology' and its application is evolving at a fast pace, and safety tools are constantly developing. This guidance will be updated to reflect significant changes in the social media environment.

[1] Home Office Task Force on Child Protection on the Internet. The taskforce aims to make the UK the best and safest place in the world for children to use the internet. It also helps protect children the world over from abuse fuelled by criminal misuse of new technologies. The Taskforce brings together government, law enforcement, children's agencies and the internet industry, who are all working to ensure that children can use the internet in safety.
http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance/

Who is this guidance for?

The guidelines have been developed for staff in County Sports Partnerships, National Governing Bodies and other organisations considering the use of social media in sport, particularly:

- people responsible for promoting sporting opportunities to children and young people
- people with designated responsibility for safeguarding children
- communications and marketing managers
- IT managers and webmasters.

These are the key people who will be involved in taking forward your organisation's involvement with social media and they will need to work together to ensure that the necessary safeguarding measures are in place and followed on a day to day basis. It is important that your organisation takes ownership for safeguarding children and young people online and takes steps across the organisation to ensure safeguarding strategies, policies and procedures address online safety issues.

What are the potential risks to children and young people using social networking and other interactive services?

With all emerging technologies there is also the potential for misuse. Risks associated with user interactive services include: cyberbullying, grooming and potential abuse by online predators, identity theft and exposure to inappropriate content including self-harm, racist, hate and adult pornography.[2]

The Byron Review sets out the risks to children posed by the internet and illustrated by the following grid.[3]

	Commercial	Aggressive	Sexual	Values
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

Most children and young people use the internet positively but sometimes behave in ways that may place themselves at risk. Some risks do not necessarily arise from the technology itself but result from offline behaviours that are extended into the online world, and vice versa. Potential risks can include, but are not limited to[4] :

- bullying by peers and people they consider 'friends'
- posting personal information that can identify and locate a child offline

[2] EUKidsOnline project : Hasenbrink, Livingstone, Haddon, Kirwil and Ponte

[3] The risks to children and young people face from the internet and video games were subject to an independent review during 2008 and the government has set up the UK Council to take forward the recommendations of the "Safer Children in a Digital World: the Report of the Byron Review". See www.dcsf.gov/byronreview/2007

[4] Ref : Home Office Task Force on Child Protection and the Internet: Good practice guidelines for the providers of social networking and other user interactive services 2008

- sexual grooming, luring , exploitation and abuse contact with strangers
- exposure to inappropriate and/or content
- involvement in making or distributing illegal or inappropriate content
- theft of personal information
- exposure to information and interaction with others who encourage self harm
- exposure to racist or hate material
- encouragement of violent behaviour, such as 'happy slapping'
- glorifying activities such as drug taking or excessive drinking
- physical harm to young people in making video content, such as enacting and imitating stunts and risk taking activities
- leaving and running away from home as a result of contacts made online.

Potential indicators of online grooming and sexual exploitation of children and young people

There is also concern that the use of social networking services may increase the potential for sexual exploitation of children and young people. Exploitation can include exposure to harmful content (including adult pornography and illegal child abuse images), and encouragement for young people to post inappropriate content or images of themselves. There have also been a number of cases where adults have used social networking and user interactive services as a means of grooming children and young people for sexual abuse. The Home Office Task Force on Child Protection on the Internet[5] identifies that online grooming techniques include:

- gathering personal details, such as age, name, address, mobile number, name of school and photographs
- promising meetings with sports idols or celebrities or offers of merchandise
- offering cheap tickets to sporting or music events
- offering material gifts including electronic games, music or software
- paying young people to appear naked and perform sexual acts
- bullying and intimidating behaviour, such as threatening to expose the child by contacting their parents to inform them of their child's communications or postings on a social networking site, and/or saying they know where the child lives, plays sport, or goes to school
- asking sexually themed questions, such as 'Do you have a boyfriend?' or 'Are you a virgin?'
- asking to meet children and young people offline
- sending sexually themed images to a child, depicting adult content or the abuse of other children
- masquerading as a minor or assuming a false identity on a social networking site to deceive a child

[5] For further information on sexual exploitation of children and young people online see the Home Office Task Force on Child Protection and the Internet: Good practice guidelines for the providers of social networking and other user interactive services 2008

- using school or hobby sites (including sports) to gather information about a child's interests likes and dislikes. Most social networking sites set a child's web page/profile to private by default to reduce the risk of personal information being shared in a public area of the site.

Good practice guidelines for sports organisations

The following guidelines contain practical safety measures for sports organisations and provide a useful starting point to help you develop an online safeguarding strategy. Organisations should ensure that all areas identified are addressed.

Planning your social media strategy

Think about your objectives

Your first steps are likely to be to:

- assess what you want to achieve with social media and how ready you are to go ahead
- decide whether you are principally aiming to interact with users, or publish information, or both
- consider which types of digital media you want to use and how to integrate them with traditional media. See Sport England's guide to Effective Signposting for more details
- consider the potential safeguarding implications of the chosen medium.

Review your existing safeguarding policies and procedures

Review your existing safeguarding policies and procedures to ensure that they address online safeguarding issues, including the potential risks to children and young people online, sexual exploitation, online grooming and cyberbullying. Remember that personal and group disputes can easily overspill from the offline to the online world.

Decide who will manage your social media

Decide who will be responsible for setting up, managing and moderating (overseeing/reviewing/responding to posted content) your web page or profile. This person will oversee the content that will appear, will decide which links to other sites to accept, and will have online contact with the children and young people who interact with your webpage or profile.

Vet and train your social media manager

You must ensure that you:

- Assess the suitability of the person who will manage your social media, including undertaking an enhanced level CRB check.
- Register that person with the new Independent Safeguarding Authority (ISA).
- Ensure the person accesses recognised safeguarding or child protection training that addresses online safeguarding issues, including warning signs of grooming and sexual exploitation.

Get to know the service you want to use

Once you've identified the service you want to use (e.g. Facebook), make sure you're up to speed with the way this service operates, and the potential safeguarding implications for children, young people and staff ***before*** setting up your sports presence. Specifically, you should look at privacy and safety tools, the terms of service (these will usually cover acceptable and unacceptable behaviour), and how users can contact the service if they have a concern or complaint. (For more details, please see the section on 'Features of social networking services' on page 17)

Integrate online safeguarding into your existing safeguarding strategy

Add online safeguarding issues to your current strategy, policies and procedures for safeguarding and child protection, retention and management of personal information, use of photographs, and codes of conduct/behaviour. Organisational reporting procedures should also include the reporting of potentially illegal/abusive content or activity, including child sexual abusive images and online grooming.

Setting up your social networking page

Use an official sports organisation email address

When you create a profile on a networking site such as Facebook, use an official sports organisation email address rather than a personal email address (e.g. joebloggs@swimming association.co.uk rather than joebloggs@hotmail.com). This will reduce the risk of impostor or fake profiles, and is important in relation to any liability or risk for the individual who sets up the profile on behalf of the organisation. Similarly, ensure that only organisational rather than personal email addresses are made available on or through a profile.

Keep your log-in details secure

Keep the log-in details to the account (including the password to the account and webpage/profile) secure within your sports organisation. This will reduce the risk of someone hacking into your online information.

Set the appropriate privacy levels

Consider the privacy and safety settings available across all aspects of the services – for photos, blog entries and image galleries - and set the appropriate level of privacy. Think about your target audience and who you wish to see the content. Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have a chance to remove them. This may result in significant personal distress, risk to the reputation of the individual, the sport and/or the organisation, and require the intervention of the organisation, the service providers and possibly the police.

Set the 'Accept comment' setting so you can check messages

The 'Accept comment' setting allows a user to approve or pre-moderate a comment from another user, usually a 'friend', before it appears on their web page/profile. Ensure that you check all messages before they appear on your sports webpage / profile so you can block any inappropriate messages and, if necessary, report them to the service provider. This may not be possible with all

social networking services. If so, you could contact the service provider to establish whether you can adjust the privacy and safety settings to suit your needs.

Include details so people can contact you directly

Put information on your web page/profile about how to contact your organisation directly, including a website address and telephone number. This allows users to get in touch and verify your sports organisation. By including details of membership of sports associations, you will also enable people to see that you are a bona fide organisation.

Promote your social networking page on your sports website

Put the web address of your social networking web page/profile on your organisation's sports website. This will help users to find your social networking page and will reduce the risk of people finding fake profiles. Take care to avoid targeting or encouraging potential users who are likely to be under the minimum age for the service.

Register as a charitable organisation with your service provider – if appropriate

Once you have set up your sport web page/profile and are adding content, it may be useful to contact the service provider. Some service providers 'register' a range of charitable organisations. This can ensure that a profile is not deleted as potentially fake or in breach of the provider's own safety policies. For example, an 'adult' profile with a number of children and young people linked as 'friends' may raise concerns on the part of the service provider about online grooming activity.

Promoting safety online

Don't target underage children

When you're promoting your sports web page/profile, don't target children who are likely to be under the minimum requirement age for the social networking service – which is usually 13 years (check this with the service provider).

Don't accept 'friend' requests from underage children

You may wish to check a user profile before accepting them. Don't accept 'friend' requests from children under the minimum age for the service – which is usually 13 years. Report underage users to the service provider and to the young person's parents (possibly via your organisation's designated person).

Avoid taking personal details of children and young people.

Don't ask users to divulge any personal details - including home and email addresses, schools or mobile numbers - that may help locate a child.

Be careful how you use images of children

Photographs and videos of children on sporting websites can be used to identify children and make them vulnerable to people who wish to groom them for abuse. To counteract this risk, the NSPCC's Child Protection in Sport Unit advises developing a policy for use of images of children that includes a procedure for reporting inappropriate images. In brief

- consider using models or illustrations to promote an activity
- if a child is named, avoid using their image
- if an image is used, avoid naming the child
- obtain children's and parents' written consent to use photographs on websites.

For more details and a sample photograph permission form, see the CPSU briefing on Photographs and Images of Children.

Remind people to protect their privacy online

Make sure that anyone using the networking site (adults and young people) are aware of the need to protect their own privacy online. They should understand the risks in posting and sharing content which may subsequently damage their reputation before they link their web page/profile to the sports profile.

Once information and images are posted online, the individual has little or no effective control of them. By the nature of social networking this content may be accessible well beyond the perceived boundaries of the organisation's site. It may also be very difficult to ensure that users' posted content and communication is restricted to the intended organisational focus (ie sport/activity matters). There are real challenges in managing a mix of sports-related content and other personal information, images and views posted by young people linked as 'friends' to the sports organisation through the social networking site. Organisations should ensure that clear guidelines for appropriate use of the site are communicated to all staff and users, and that any settings or filters to restrict unwanted postings are applied.

Think before you post

Ensure that any messages, photos, videos or information comply with existing policies within your organisation. Ask yourself whether photographs or text are appropriate to your target audience, and if they may create any potential safeguarding concerns. Always seek the permission of young people and their parents before adding photos of or information about children or young people to your sports web page/profile.

Promote safe and responsible social networking

Promote safe and responsible use of social networking to your sports audience online. You could do this by uploading safety videos, messages or links onto your sports web page/profile. If you do not yet have a safe and responsible use policy or safety tips for your sport, see the 'Sources of information' section at the end of this document on page 22.

Provide links to safety and support organisations

Provide links to safety and support organisations on your profile. Or, better still, accept these organisations as 'friends' so that they appear on your sport web page/profile in the 'Friends' section.

Data Protection considerations

Take care when advertising sporting events and competitions online when you are collecting personal information about users, including children and young people. In these circumstances, you should follow the requirements concerning the collection of personal information, as set out in the Data Protection Act 1998. You can use social media without collecting personal data outside of the service you are using and you should consider this alternative.

Beware of fake celebrity sports profiles

It has been known for fake or impostor profiles of famous sports people to appear on social networking services. Sometimes people use these fake profiles to groom children by seeking to gain their trust and attempting to set up a meeting offline. Fake profiles may be intended to be fun, however they can be set up with malicious intent to ridicule or harass an individual. Before linking to a celebrity sports profile, contact the sports person offline and check the address of their official web page/profile.

Reporting problems

Reporting concerns about possible online abuse

All staff should be familiar with your organisation's reporting procedures which should include the reporting of potentially illegal/abusive content or activity, including child sexual abusive images and online grooming. In addition to referring concerns to your organisation's designated person, you should immediately report online concerns to the Child Exploitation and Online Protection Centre (CEOP) or the police, in line with internal procedures. Law enforcement agencies and the service provider may need to take urgent steps to locate the child and/or remove the content from the internet.

In the UK, you should report illegal sexual child abuse images to the Internet Watch Foundation at www.iwf.org.

Reports about suspicious behaviour towards children and young people in an online environment should be made to the Child Exploitation and Online Protection Centre at www.ceop.uk.

Where a child or young person may be in immediate danger, always dial 999 for police assistance.

See the section on 'Sources of information' for more details on page 22.

Reporting other breaches of terms of service

If you have concerns about inappropriate content or behaviour which potentially breaches the terms of service, you should report this to the service provider. The terms of service set out the legal conditions concerning use of the service and include the minimum age requirement. Also, an acceptable use policy usually makes clear what behaviour is and is not acceptable on the service e.g.

harassment, defamation, obscene or abusive language, and uploading material which is libellous, defamatory, obscene, illegal or violent or depicts nudity. See the section on 'Features of social networking' for more details on page 17.

Working with a digital agency

Depending upon the size of your organisation, you may wish to engage a specialist social media company to analyse the market, optimise your audience, keep your online content fresh and moderate your webpage/profile. Here are some points to bear in mind when working with an external web agency.

Ensure your web agency moderator passes safety checks

Your web agency may offer to moderate your web page/profile on your behalf. The person who moderates your profile must:

- be appropriately selected, including a Criminal Records Bureau (CRB) check.
- be registered with the new Independent Safeguarding Authority (ISA).

If the web agency is based outside the UK, ask if they have equivalent legislation or guidelines or if they follow the principles of UK law and guidance.

Ensure your web agency moderator follows good practice guidance

The person at the web agency who acts as a moderator for your web page/profile should also follow Home Office good practice guidance for moderating interactive services for children. See the 'Sources of information' section for more details on page 22.

Involve your designated safeguarding person

When you engage a social media company to manage and moderate your web page/profile, it's important that you also involve the designated person for safeguarding children within your organisation. Your internal designated person should take responsibility for ensuring that any online safeguarding concerns are handled in line with your existing safeguarding policies and procedures.

Ask to see the company's safety and privacy policies

When contracting or outsourcing social media work, ask to see the organisation's safety and privacy policy. This should cover: safety tools that are in place; safe use guidelines and complaints reporting procedures; relevant criminal record checking procedures for moderators; and adherence to relevant legal or good practice guidance.

Ensure the agency follows internet advertising best practice

Some companies collect and use data for online advertising purposes. This is a growing practice known as online behavioural advertising and involves the delivery of relevant advertising to groups of anonymous web users, based upon previous internet browsing activity.

Recent good practice guidance produced by the social media industry (Internet Advertising Bureau) recommends that companies should not create or sell online behavioural segments intended for the

sole purpose of targeting children they know to be under 13. The guidance sets out core commitments about providing notice, giving choice and educating consumers about how data will be collected. It also covers personally identifiable information which uniquely identifies an individual offline.

Engaging with a social networking service provider

Make sure the service provider follows legislation and good practice

When you engage with a social networking agencies it's important to ensure it adheres to relevant legislation and good practice guidelines.

In the UK this means:

- following good practice guidelines from the Home Office Task Force on Child Protection on the Internet on chat, instant messaging, web-based services, moderation, safe search, social networking services and other user interactive services
- following the requirements of the Data Protection Act 1998 on collection and use of personal data
- carrying out criminal record checks where moderators are used on services likely to attract children, in accordance with the Safeguarding Vulnerable Groups Act 2006.

If the company is based outside the UK, ask if they have equivalent legislation/guidelines or if they follow the principles of UK law and guidance.

For more information, please see the section on 'Sources of information' on page 22.

What is social media?

'Social media' refers to the latest generation of interactive online services such as blogs, discussion forums, podcasts and instant messaging. Social media includes:

- social networking sites e.g. Bebo, Facebook, Piczo, Hi5 and MySpace
- micro-blogging services e.g. Twitter
- video-sharing services e.g. YouTube
- photo-sharing services e.g. Flickr
- online games and virtual reality e.g. Second Life.

You should refer to the Features of Social Networking Services section for more information on some of the common features that most social networking and interactive services have.

Social media is a dynamic, constantly-evolving form of communication that allows people to take part in online communities, generate content and share information with others. Users can now access interactive services across a multitude of services and devices, such as mobile phones, personal digital assistants (PDAs), game consoles and personal computers.

Social media services are particularly popular with children and young people, as they offer them opportunities to be creative, connect with others all over the world and share interests. The Home Office report on Child Protection on the Internet says that social media allows users to:

- create and design a personal webpage / profile which is integrated into the social networking site using graphics, colour, music and images to represent the user's unique style and identity
- interact with friends in real time through instant messaging, message boards and chat rooms that are integrated into the social networking site
- meet known friends and make new friends
- link to friends' personal web pages/profiles which are integrated into the social networking site
- upload and share images of themselves, their family and friends
- upload and share videos
- create blogs, journals or diaries about their lives
- publish and share their own music
- share thoughts and information on areas of interest
- play online games
- receive comments or messages on their personal web page/profile from friends or guests
- create or join wider communities or interest groups e.g. music, sport
- complete or create questionnaires integrated into some social networking services.

The benefits of engaging with social media

Social media provides a range of unique opportunities for sports organisations. It can help you:

- promote the benefits of fitness and sport to all children and young people and it should be a route to the semi sporty and hard-to-reach groups too
- engage, connect and develop unique relationships with young people in a creative and dynamic medium where users are active participants
- disseminate messages about events or campaigns virally among supporters in online communities.

A sports club could set up a page that communicates with club members about training schedules, competitions and events. The aim is to create a sense of community and involvement.

Commercial organisations have come up with some iconic examples that show the power of engaging people in sport through social media. Within Facebook, Nike have set up the Nike Women's page that provides an area for the brand and women to share their experiences of fitness and running with various applications included to help deliver functional and useful products to help their participation in sport. Another site that targets running enthusiasts is http://www.mapmyrun.com/. It has created a successful fitness community where people talk about running, set goals and exchange advice.

Meanwhile, at http://www.realbuzz.com/, people can learn about health and fitness, find out about a variety of sports, triathlons and charity challenges, take part in forums and blogs, and share recommendations and tips with like-minded people.

Successful social media sites connect with people's passion for sport, give people a chance to participate – whether that's uploading a video, commenting on a blog or tracking their progress, and create vibrant online communities.

For more ideas on the possibilities of social media, please see the Sport England 'Effective Signposting' report. This talks about how to involve children and young people in sport through your communications. Here are three tips from the report that relate to social media:

1. Use traditional methods – posters, demos and young sporting ambassadors – to attract attention, then use digital communications to spread word-of-mouth recommendations and retain young people.
2. Digital communications are best if they reinforce a real relationship.
3. The best web sites are frequently updated, use incentives to encourage people to engage (e.g. reduced club membership and sporting equipment), allow people to have an input, and make users feel part of a community.

It is important for organisations to give careful consideration to the use of social media in sport and to balance the benefits of creativity, spontaneity and immediacy of the communication with the potential risks, including the risks to children. You should only move forward with developing social networking sites when safeguarding issues have been adequately assessed and addressed to minimise these potential risks.

Features of social networking services

Common features of social networking and user interactive services include:

- *A minimum age requirement.* Many social networking services set 13 years of age as the minimum age at which a young person can register as a user of the service. This is because many of the social networking services are based in the US and are required to comply with US law which designates the age of 13 to protect children's privacy online, including their personal information. The US law covers companies providing services in the US and overseas.[6]
- *Commercial advertising.* Commercial advertising may appear on various parts of the website. Commercial advertising on social networking sites is usually displayed to ensure that it is appropriate for the likely audience. If the service is aimed at, or likely to attract, users under the age of 18, social network service providers must follow relevant guidelines or codes for advertising to minors.[1] It is important for children and young people to enter their correct age so social networking service providers can ensure that steps are taken to display advertising to the appropriate audience.
- *Terms of service.* The terms of service set out the legal conditions concerning use of the service including the minimum age requirement. An acceptable use policy is usually included and this makes clear what behaviour is and is not acceptable on the service i.e. harassment, defamation, obscene or abusive language, the uploading of material which is libellous, defamatory, obscene, illegal or violent, or depicts nudity etc. Sanctions for misuse include deletion of an account and/or co-operation with law enforcement. The terms of service are usually found by clicking through the tab at the bottom of the homepage of the site.
- *Registration process.* Most social networking services have a registration process. This is an important step for authenticating user identification and usually involves the user providing an email address and the service sending an email to that address to enable the registration process to continue. Registration is also an important step for promoting safe and responsible behaviour online. Users are asked to provide a certain amount of personal data and agree to the terms of service. The service provider should give information about how the data collected in registration will be used, including what information will appear on their website/profile, and what will be private. Some social networking sites provide online registration tutorials on the site to help new users set up an account and profile safely.

[6] In the UK this is the British Code of Advertising, Sales, Promotion and Direct Marketing. www.cap.org.uk

- *Privacy and safety tools.* Most social networking services provide privacy and safety tools to enable users to manage 'who sees what' and who they interact with on the service. These tools include 'block/remove this user', 'flag inappropriate content' and 'report user/abuse' to the moderator/service and can feature in some or all aspects of the service for such things as journals, blog entries and image galleries. Privacy and safety tools are usually part of a user's account, accessible every time a user logs in.
- *Safety warnings and information.* Many social networking services provide safety warnings and advice at different stages of the service. This can begin at the initial registration stage when users are asked to provide a certain amount of personal data and agree to the terms of service. Safety warnings can appear every time a user uploads a photo to their web page/profile. For example: 'Photos may not contain nudity, violent or offensive material, or copyrighted images. If you violate these terms, your account may be deleted'. Safety advice and links to safety resources can be found on many social networking services sites, usually by clicking on a safety link at the bottom of every page.[7] Some social networking services provide online safety tutorials on their sites.
- *Moderation.* Moderation is an activity or process whereby a person and/or technical filters are responsible for reviewing content posted by users[8]. Moderation is usually undertaken according to an agreed set of guidelines or terms of service and includes what is acceptable and unacceptable behaviour on the site or within the online community. The use of moderation by social networking and interactive services poses a challenge to social networking and interactive services where millions of users generate and upload a considerable amount of content, including images, video footage and messages, on a continuous basis. Some service providers utilise a mix of technical filters, human moderators and also rely upon users to report content, using a 'Flag content as inappropriate' button to make a report to the service.
- *Reporting concerns.* Many social networking services provide a complaints process. The complaints process gives users the option to report matters that concern them. This could range from offensive communications which breach the provider's terms of service to potentially illegal activities. They might include posting images depicting child abuse images, suspicious behaviour towards children and young people indicative of grooming, bullying and harassment, and other potentially illegal or criminal behaviour. The 'report concerns' process is usually available by clicking on a 'Contact us' link at the bottom of every page on the site. Many social networking services work towards responding to complaints within a set period of time e.g. 24hrs.

What does a user's webpage / profile contain? A user can upload all kinds of information onto their webpage / profile for others to see. This can include personal information about their likes, dislikes, music tastes, favourite films, images including photos (including photos taken on a mobile phone camera), and videos including webcam. Photos can be uploaded onto the webpage / profile or a user may also decide to feature other photos, videos or blogs in their Photos, Videos and Blogs sections. A user can invite other 'friends' to feature their webpage / profile and the top 'friends' profiles will appear on a dedicated section of the webpage / profile. A user's webpage / profile can also have a section for

[7] The Home Office Task Force on Child Protection on the Internet: Good practice guidance for the providers of social networking and other interactive services 2008 contains a set of safety recommendations which service providers are encouraged to adopt are support a safer environment for young users.
[8] Ref: Home Office Task Force on Child Protection on the Internet: Good practice guidance for the moderation of interactive services for children 2005

comments from friends and a user can set their privacy setting to pre-moderate these comments before they appear on the page / profile.

Social media, the law and good practice guidance

Here's a summary of some of the laws and guidance that protect children and young people from the potential risks of social media.

Online advertising to children

Depending upon the size of your organisation, you may wish to engage with a specialist social media company. These companies help brands analyse the market, optimise your audience, keep your content online fresh and moderate your web page/profile. Some companies collect and use data for online advertising purposes. This is a growing practice known as online behavioural advertising and involves the delivery of relevant advertising to groups of anonymous web users, based upon previous internet browsing activity.

Recent good practice guidance produced by the social media industry (Internet Advertising Bureau[9]) recommends that companies should not create or sell online behavioural segments intended for the sole purpose of targeting children they know to be under 13 years. The guidance also sets out core commitments about providing notice, giving choice and educating consumers about how data will be collected. Personally identifiable information which is data that, by themselves or in conjunction with other data held uniquely identifies an individual offline is also covered. See Sources of Safety Advice and Information.

Moderators

Social media and moderation companies may also offer to moderate your webpage/profile on your behalf. This involves assigning a person to moderate or manage the interaction with users on the webpage/profile. This person, sometimes referred to as a moderator, is most likely to have online contact with younger users interacting with the webpage/profile. You should ensure that this person is CRB checked/registered with the new Independent Safeguarding Authority (ISA)[10]. If the company is based outside of the UK i.e. based in the US, ask if they have equivalent legislation/guidelines or if they follow the principles of UK law and guidance.

The Home Office good practice guidance for the moderation of interactive services for children sets out recommendations for those providing moderation services aimed at or likely to attract children[11]. This includes the warning signs of online grooming. Also see section above on potential risks to children and online grooming and sexual exploitation of children and young people online.

---

[9] Ref : See Internet Advertising Bureau for further information

[10] The Safeguarding Vulnerable Groups Act 2006 includes moderators who have responsibility for interactive services and is due for implementation in Oct 2009. See Appendix

[11] The Home Office Task Force on Child Protection on the Internet: Good practice guidance for the moderation of interactive services for children provides information and recommendations for the moderation of interactive communication services aimed at or very likely to attract children in the following areas :

- Information and advice to users
- Risk assessment
- Recruitment
- Training
- Data security
- Management and supervision and
- Escalation procedures

When engaging with social networking companies (e.g. Facebook, Bebo or MySpace) it is important to ensure that they adhere to relevant legislation and good practice guidelines

If the company is based outside of the UK e.g. based in the US, ask if they have equivalent legislation/guidelines or if they follow the principles of UK law and guidance.

When contracting or outsourcing this work ask to see the organisation's safety and privacy policy which could include: safety tools in place; safe use guidelines and complaints reporting procedures; relevant criminal record checking procedures for moderators; and adherence to relevant legal or good practice guidance.

UK legislation and good practice guidelines

Home Office Task Force on Child Protection and the Internet: Good practice guidelines on chat, instant messaging, web based services, moderation, safe search and social networking services and other user interactive services.

Home Office Task Force on Child Protection on the Internet: Good practice guidance for the moderation of interactive services for children provides information and recommendations in the following areas for the moderation of interactive communication services aimed at or very likely to attract children:

- Information and advice to users
- Risk assessment
- Recruitment
- Training
- Data security
- Management and supervision and
- Escalation procedures

The new Independent Safeguarding Authority

The Independent Safeguarding Authority (ISA) is responsible for the new Vetting and Barring Scheme (VBS) which will be fully operational in November 2010. Created under the Safeguarding Vulnerable Groups Act 2006, it replaces the current List 99 and Protection of Children Act List which debar certain individuals from working (on a paid or unpaid basis) with children and young people. When the scheme is operating, It will be illegal to hire someone in a regulated position or regulated activity who is not a member of the scheme, and has therefore not been checked by the ISA. The new scheme will eventually cover the entire children's workforce - some 11.3 million people.

The ISA will assess people using data from various agencies, government departments and the Criminal Records Bureau (CRB).

The Act introduces a new legal requirement for social network site moderators. Registration with the ISA will be mandatory for individuals with specific responsibilities in relation to online interactive services and sites, who:

- moderate a public electronic interactive communication service used wholly or mostly by children

- have access to content
- monitor content which forms part of the service
- remove matter, or prevent addition of matter to, the service
- control access to, or use of, the service
- have contact with users of the service.

The Data Protection Act

According to the Data Protection Act 1998, people must give consent to the processing of their personal data on a website.

The act doesn't give specific guidance on obtaining permission from children. However, in the note on 'Collecting personal information using websites', the Information Commissioner makes the following comments:

- Websites that collect information from children must have stronger safeguards in place to make sure any processing is fair.
- Notices explaining the way you will use children's information should be appropriate to their level, and should not exploit any lack of understanding.
- 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.

US privacy law

The US has a special law that applies to children and online privacy. According to the Children's Online Privacy Protection Act (COPPA) of 1998, commercial websites directed at children under the age of 13 must obtain verifiable consent from a parent before collecting, using or disclosing personal information from a child. For this reason, many US websites prohibit children under 13 from registering or using their sites.

Sources of information

The government, law enforcement services, children's charities and industry representatives have developed a range of safety materials to encourage safe and responsible use of the internet. Many of these resources are available online to download.

Byron Review

The Government commissioned the Byron Review to look into internet-related risks for children. The result is the report: 'Safer Children in a Digital World'.
http://www.dcsf.gov.uk/byronreview/

Child Exploitation and Online Protection Centre (CEOP)

The CEOP is a police organisation concerned with the protection of children and young people from sexual abuse and exploitation, with a particular focus on the online environment. It also runs an education programme called 'Thinkuknow' for professionals to use with children and young people to help keep them safe online.

In association with the Virtual Global Taskforce, an international group of agencies that tackle abuse, CEOP provides an online facility for people to report sexually inappropriate or potentially illegal online activity towards a child or young person. This might include an adult who is engaging a child in an online conversation in a way that makes the child feel sexually uncomfortable, exposing a child to illegal or pornographic material, or trying to meet a child for sexual purposes.

Where a child or young person may be in immediate danger, always dial 999 for police assistance.

www.ceop.gov.uk
www.thinkuknow.co.uk

Childnet International

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

www.childnet-int.org

ChildLine

ChildLine is a service provided by the NSPCC that offers a free, 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

Data Protection and the Information Commission Office

The Information Commissioner's Office has a range of information and guidance on people's rights, responsibilities and obligations related to data protection.
'Keeping your personal information personal' is a guide for young people on looking after their personal information on social networking sites.
http://www.ico.gov.uk/Youth/section2/intro.aspx

'Collecting personal information from websites' is a guide to collecting information online. It includes a section on collecting information about children, publishing information about children and parental consent.
http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.0.pdf

www.ico.gov.uk

EU Kids Online project

The EU Kids Online project (2006-2009) examines children's safe use of the internet across 21 countries.

http://www.lse.ac.uk/collections/EUKidsOnline/

Home Office Taskforce on Child Protection on the Internet

The Home Office Taskforce on Child Protection on the Internet is an authoritative source of information on helping children stay safe online.

Social Networking Guidance

http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance/

Guidance for the Moderation of Interactive Services for Children

http://police.homeoffice.gov.uk/publications/operational-policing/moderation-document-final.pdf
http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce

Good Practice Models and Guidance for the Internet Industry on Chat Services, Instant Messaging and Web-based Services

http://police.homeoffice.gov.uk/publications/operational-policing/ho_model.pdf

The Internet Advertising Bureau

The Internet Advertising Bureau has guidelines on online advertising.

www.iabuk.net

Child Protection in Sport Unit (CPSU)

The CPSU provides a range of services to support partners in the sports sector including:

- safeguarding briefings and updates
- development and delivery of training and learning resources
- supporting organisations to put effective systems and structures in place.

www.thecpsu.org.uk

CPSU Briefing on Photographs and Images of Children

The NSPCC's Child Protection in Sport Unit (CPSU) has created a briefing that gives guidelines on using photographs of children and has a sample permission form for children and parents.

http://www.nspcc.org.uk/Inform/cpsu/Resources/Briefings/PhotographsAndImagesOfChildren_wdf60645.pdf

Cyberbullying

The Teachernet site has a wealth of information on cyberbullying.

www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/

Internet Watch Foundation

The Internet Watch Foundation (IWF) 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. The IWF works in partnership with the online industry, the Government, law enforcement agencies and other hotlines abroad to remove such content from

the internet. A prominent link for reporting illegal content appears on the home page of the IWF website.

www.iwf.org.uk

Teachtoday

'Teachtoday' provides resources for teachers on the responsible and safe use of new and existing communications technologies. It aims to help schools:

- understand new mobile and internet technologies, including social networking
- know what action to take when facing problems
- find resources to support the teaching of positive, responsible and safe use of technology.

www.teachtoday.eu

Sign up now to the CPSU E-Newsletter - We can email you the latest information about child protection in sport, simply e-mail the word subscribe to cpsu@nspcc.org.uk

(September 2009)