

Using Social Networking Services and Social Media: Promoting Safe and Responsible use

Contents

- [Executive summary](#)
- [Purpose of guidance](#)
- [Who is the guidance for?](#)
- [Opportunities that social media offers sports organisations](#)
- [Potential risks to children and young people using social networking and other interactive services](#)
- [Potential indicators of online grooming for abuse](#)
- [Good practice guidance](#)
- [Appendix A:](#) Information about Social Networking Services and Social Media
- [Appendix B:](#) Sources of further information and guidance

Executive summary

As County Sports Partnerships and National Governing Bodies become increasingly adept at communicating with young people it is critical that safeguarding protocols keep pace with the raft of communication methods young people use.

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

- Understand the safety aspects including what is acceptable and unacceptable behaviour on a social networking service.
- Your organisation should follow relevant legislation and good practice guidance when engaging with social media companies.
- 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.
- Ensure that online safeguarding issues are fully integrated into your existing safeguarding strategy, policies and procedures.
- Decide how your sports webpage/profile will be managed within your sports organisation.
- Registration or 'signing up' your sports club/organisation.
- Privacy and safety settings.
- Ensure that staff and volunteers, including coaches and athletes are aware of the need to protect their privacy online.
- Address safety when adding content to your webpage/profile.
- Promote your sports webpage/profile.
- Contacting the social networking provider.

Purpose of this guidance

This CPSU 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 local clubs considering or already engaged in the use of social 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 sports presence 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 document has been produced to reflect the current good practice guidance produced by the Home Office Task Force on Child Protection¹ 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.

Who is this guidance for?

This briefing will be useful for all those involved in an organisation considering the use of social media in sport. 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. This guidance specifically targets the following people in your organisation:

- The lead officer responsible for promoting sporting opportunities to children and young people
- Designated person responsible for safeguarding children
- Communication and/or marketing person
- IT manager and /or webmaster

These are the key people who will be involved in taking forward your organisation's involvement in 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.

What opportunities does the use of social media offer sports organisations?

Social networking services allow users to create their own content and share it with a vast network of individuals sometimes referred to as online communities. People from all over the world can meet and share interests online. There are several hundred social networking services. Some examples of popular services include: Bebo, Facebook, Flickr, Piczo, Hi5, MySpace and Twitter. Other services focus on video sharing and include Youtube.

Social media provides unique opportunities for sports organisations to engage, connect and develop unique relationships with people in a creative and dynamic medium where users are active participants. Information about an event or campaign messages can be dissipated virally amongst supporters within online communities.

Many people are already initiating their own discussion about sport in blogs, forums, groups, uploading a sports video clip on to their social networking webpage/ profile and bookmarking to share with others. For example, there are numerous video clips of Usain Bolt breaking the world record in the 100m at the Beijing Olympics on YouTube. These video clips have been uploaded by users, some with up to 450,000 views and various comments from other users on those last 10- 20 metres.

¹[The Home Office Task Force on Child Protection website.](#)



Sport England has produced 'A guide to effective signposting to children and young people'. This guide assists organisations in using a range of communication tools to effectively signpost children and young people to sporting opportunities.

It is important for organisations to give careful consideration to the use of social media in sport and balance the benefits of creativity, spontaneity and immediacy of the communication with the potential risks, including the risks to children (For further information see page 6, part 4. Ensure that online safeguarding issues are fully integrated into your existing safeguarding strategy, policies and procedures).

Your sports organisation will need to make decisions about:

- how to best present its activities online
- what type of content to upload (e.g. photos, blogs, video clips, podcasting, slide shows, discussion groups)
- allowing users to paste content from your webpage on to their own personal webpage/ profile and share with others
- how to interact with users in such a dynamic environment.

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: cyber bullying, grooming and potential abuse by online predators, identity theft and exposure to inappropriate content includes self-harm, racist, hate and adult pornography.²

The Byron Review sets out the risks to children posed by the Internet and illustrated by following the grid below.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	'Sexting' - 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

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

³The 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 <http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews>.



behaviours that are extended into the online world, and vice versa. Potential risks can include, but are not limited to⁴ :

- Bullying by peers and people they consider 'friends';
- Posting personal information that can identify and locate a child offline;
- 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; and
- 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 capabilities 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. 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. Online grooming techniques include⁵:

- 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;
- 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 webpage/profile to private by default to reduce the risk of personal information being shared in a public area of the site.

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

⁵For 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



Good practice guidelines for the safe use of social media

The following guidelines contain practical safety measures to sports organisations and provide a useful starting point for the development of your organisation's online safeguarding strategy. The guidance is not listed in a set order or sequence, and organisations should ensure that all areas identified are addressed.

Your organisation has identified the need to communicate effectively with children and young people and you are considering the use of social networking services as part of your overall communication strategy. Some steps to take at this stage are to:

- Assess your business needs and readiness
- Consider what your objectives for use are e.g. interaction with users, publishing, or a mix of both
- Consider the medium that you want to use or the blend of mediums as detailed in Sport England's "A Guide to Effective Signposting for Children and Young People"

You may wish to explore social networking services and carry out further research to help inform your decision. If you decide to use social networking services then use the following safeguarding checklist.

1. Understand the safety aspects including what is acceptable and unacceptable behaviour on a social networking service

Become familiar with user interactive services **before** setting up your sports presence on a social networking or other interactive service. This should specifically include privacy and safety tools, the terms of service (the terms of service usually contain what is acceptable and unacceptable behaviour), and how users can contact the service if they should have a concern or complaint. See Appendix A: Information about social networking and social media?

2. Your organisation should follow relevant legislation and good practice guidance when engaging with social media companies

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 webpage/ 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 Bureau⁶) recommends that companies should not create or sell online behavioural segments intended for the sole purpose of targeting children they know to be under 13yrs. 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 Appendix B: Sources of Safety Advice and Information.

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 as part as safe recruitment process (also see CPSU briefing on Safe recruitment and selection procedures- http://www.nspcc.org.uk/Inform/cpsu/resources/briefings/safe_recruitment_and_selection_procedures_wdf67399.pdf). 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.

⁶Internet Advertising Bureau visit - www.iabuk.net



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 children⁷. This includes the warning signs of online grooming. Also see previous section on potential risks to children and online grooming and sexual exploitation of children and young people online.

3. 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

In the UK this includes:

- 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. See Appendix B: Sources of Safety Advice and Information
- Collection and use of personal data and the Data Protection Act 1998. See Appendix B: Sources of Safety Advice and Information
- Having safe recruitment processes for moderators of social networking site that involve children and young people.

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.

4. Ensure that online safeguarding issues are fully integrated into your existing safeguarding strategy, policies and procedures

Adhere to good practice guidelines

Ensure that the sports webpage/profile adheres to existing good practice policies including safeguarding and child protection, privacy of personal information, the use of photographs and acceptable behaviour.

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

Review 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 overflow from the offline to the online world.

Reporting online concerns about possible abuse

Organisational reporting procedures should include the reporting of potentially illegal/abusive content or activity, including child sexual abusive images and online grooming. In addition to referral to the organisation's designated person, concerns arising online should be reported to Child Exploitation and Online Protection Centre (CEOP) or the Police immediately 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.

⁷Home Office Task Force on Child Protection and the Internet: Good practice guidelines for the providers of social networking and other user interactive services 2008.



In the UK, illegal sexual child abuse images should be reported to the Internet Watch Foundation at www.iwf.org. See Appendix B: Sources of Safety Advice and Information

Reports about suspicious behaviour towards children and young people in an online environment should be made to the Child Exploitation and Online Protection Centre (CEOP) at www.ceop.police.uk. See Appendix B: Sources of Safety Advice and Information.

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

Reporting other breaches of terms of service

Concerns about inappropriate content or behaviour which potentially breaches the terms of service should be reported to the service provider. 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, nudity, violent etc. See Appendix A: What is social networking and social media?

5. Decide how your sports webpage/profile will be managed within your sports organisation

Management of the profile

Decide who will have responsibility for: the setting up, management, and moderation (overseeing, reviewing and responding to posted content) of the webpage/profile. This includes the content you upload to appear, what you accept to be linked to your webpage/profile, and the communication or interaction with users. This person is most likely to have online contact with younger users, interacting with the webpage/profile; therefore there should be some level of accountability and support from the organisation.

Vetting and training

This person should be appropriately vetted and receive recognised safeguarding or child protection training. Training should also address online safeguarding issues, including what warning signs to look out for. See information above on *potential risks to children and young people* using social networking and what is grooming and sexual exploitation of children and young people online (also see CPSU understanding the grooming and entrapment process briefing-

http://www.nspcc.org.uk/Inform/cpsu/resources/briefings/understanding_grooming_entrapment_process_wdf77040.pdf)

Involve your Designated Safeguarding Person

If you are engaging a social media or moderation company to manage and moderate your webpage/profile it is important that the designated person for safeguarding children within your organisation also has responsibility for the management and moderation of the webpage/profile to ensure that any online safeguarding concerns are handled in line with your existing safeguarding policies and procedures.

6. Registration or 'signing up' your sports club/organisation:

Choose an appropriate email address to register/set up a profile/account

This requires an email address – use an official sports organisation email address rather than a personal email address (e.g. joebloggs@swimmingassociation.co.uk rather than joebloggs@hotmail.com). This will reduce the risk of the establishment of impostor or fake profiles, and is important in relation to any liability or risk for an individual/employee required to set 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.

Security

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



7. Privacy and safety settings:

Set the appropriate privacy level

Consider each of the privacy and safety settings available across all aspects of the services i.e. photos, blog entries, image galleries and set the appropriate level of privacy taking into consideration 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 it. 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.

Accept 'friends' setting and minimum user age

You may wish to check a user profile before accepting them. Do not accept friend request from children under the minimum age for the service (usually 13 years). Report underage users to the service provider and to the young person's parents (perhaps via the organisation's designated person).

'Accept comment' setting

This allows a user to approve or pre moderate a comment from another user, usually a 'friend' before it appears on their webpage/profile. Ensure that all messages are checked before they appear on your sports webpage/ profile to ensure that any inappropriate messages are blocked and if necessary reported to the service provider. This may not be possible with all social networking services. You may wish to contact the prospective service provider to establish if steps could be taken to adjust the privacy and safety settings for your needs.

8. Ensure that staff and volunteers, including coaches and athletes are aware of the need to protect their privacy online

Make sure that your staff and coaches (paid and volunteers), sports athletes, students and trainees, and are aware of the need to protect their own privacy online. They should understand the risks in posting and sharing content which may damage their reputation before they link their webpage/profile to the sports profile. See Appendix B: Sources of Safety Advice and Information

9. Address safety when adding content to your webpage/profile:

Sports contact details

Add information about how to contact your sport organisation including a website address, if available. Also include offline contact details for your club and any information on membership of a sports association. This allows users to contact your organisation directly and verify your sports organisation offline.

Promote your sports webpage/profile

Feature details of your organisation's social networking webpage/profile on your sports website. A webpage/profile address on a social networking service is sometimes referred to as the URL. This helps users to easily locate your organisation's presence online and reduce the risk of locating the wrong webpage/profile including any fake profiles. Do not target children and young people who are likely to be under the minimum requirement age for the social networking service in any promotion of the sports webpage/profile

Promote safe and responsible use

Consider promoting safe and responsible use of social networking to your sports audience online. This could include uploading safety videos, messages or links onto the sports webpage/profile. If you do not yet have a safe and responsible use policy or safety tips for your sport, there is a considerable amount of safety material available. See Appendix B: Sources of Safety Advice and Information.

Links to safety and help organisations

Provide links to safety and support organisations on the profile, or better still accept these organisations as 'Friends' so that they appear on the sport webpage/profile in the 'Friends' section. See Appendix B: Sources of Safety Advice and Information.



Sports events and competitions

Consider the integration of offline events with your sports presence online. Extra care should be taken when advertising these events online and where information about users, including children and young people is collected. In these circumstances you will need to follow the legal requirements concerning the collection of personal information, as set out in the Data Protection Act 1998. See Appendix B: Sources of Safety Advice and Information.

Avoid taking personal details of children and young people

Do not ask users to divulge personal details including home and email addresses, schools, mobile numbers that may help locate a child. It is best to provide the details of the event and signpost to where users can obtain further information e.g. further information can be obtained from your local sports organisation or club.

Uploading Content – ‘think before you post’

Consider any messages, photos, videos or information – do they comply with existing policies within your organisation? (e.g. use of photographs of children). Is the content e.g. photographs and text appropriate to the audience? Always seek young person/parental permission to use the photos of those featured before adding to the sports webpage/profile.

Fake or impostor webpage/profiles

Beware of fake or impostor profiles of well known or celebrity sports people. It has been known for fake or impostor profiles to be set up on social networking services. Sometimes this is intended to be fun, however fake profiles can be set up with malicious intent to ridicule and harass an individual. It can also be used to groom children by those seeking to gain a child's trust and attempt to set up a meeting offline. It is best to first make contact offline with the sports person and check if they have an official webpage/profile.

10. Promote your sports webpage/profile

Once you have set up the sport webpage/profile and are in the process of 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 their own safety policies e.g. 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.

You can also explore with the social networking service how they can promote your profile and help you reach new users. Social networking services are set up with various sections of interest. This can include music, comedy, events and more recently areas that promote social responsibility, inclusion, health and well being. These areas or sections are usually featured on the home page of the site with a selection of the most popular web pages/profiles. These are sometimes themed or linked to a global or national event or campaign which gives exposure to potentially millions of users worldwide.

11. Contacting the social networking provider

There is usually a ‘contact us’ at the bottom of every page with an email address to explore how they can promote your sports profile.

Remember

Setting up a presence on social media involves providing interactive content which engages and connects with people. It requires a continuous interaction with your audience or they may become bored with a ‘static’ webpage/profile.

Example: Social media in action: Nike+iPod Sports kit allows a user to set up play lists for their runs, tracks the runs, and is integrated into a Nike+ website where you can connect with others in a community and analyse your runs (visit Nike website for further information http://inside.nike.com/blogs/nikerunning_training-en_IN/2010/01/22/gait-analysis-intro)⁸.

⁸Ref :Guide to Social Media : Internet Advertising Bureau



Appendix A:

Information about Social Networking Services and Social Media

Background

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. This new communication medium is dynamic and constantly evolving.

These services are part of a significant shift in the evolution of the Internet, referred to as 'Web 2.0'.

'Web 1.0' involved static websites, download of content, use of search engines, and surfing from one website to another. 'Web 2.0' represents a significant shift away from this model, towards a more dynamic and interactive Internet. The technologies and tools available on Web 2.0 are not new but bring together existing interactive technologies on a single service. Technologies and tools available can include all or some of the following: search, email, messaging, and chat, blogs, gaming, discussion forums, Voice over Internet Protocol (VoIP), photos, music and videos.

Users are no longer passive recipients of information found on static websites but are active participants in online communities where content is generated by users and easily shared with others. User interactive services are particularly popular with children and young people offering them opportunities to be creative connect with others and share interests.

The convergence of technical and communication platforms is another significant development. Users can now access interactive services using across a multitude of services and devices, such as mobile phones, personal digital assistants (PDA's), game consoles as well as personal computers.

What are social networking and other user interactive services?

Social networking services allow users to create their own content and share it with a vast network of individuals sometimes referred to as online communities. People from all over the world can meet and share interests. There are several hundred social networking services. Some examples of popular services include: Bebo, Facebook, Flickr, Piczo, Hi5, MySpace and Twitter. Other services focus on sharing, commenting on or rating video and include Youtube.

Social networking services vary in terms of the range of services and functions offered. They can allow users to⁹:

- 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 webpage/profile 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 webpage/profile from friends or guests;

⁹Ref : 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



- create or join wider communities or interest groups e.g. music, sport ;and
- complete or create questionnaires integrated into some social networking services

What are the common features of social networking and user interactive services?

Common features of social networking and user interactive services include:

- *Minimum age requirement.* Many social networking services have 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 designate 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.¹⁰
- *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.¹⁰ This is one reason why it is important for children and young people to enter their correct age and how 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, nudity, violent 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 this is usually based upon providing an email address and an email is then sent to the email 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. 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 should be provided by the service provider. Some social networking sites provide online registration tutorials available on the site to help new users set up an account and profile safely.
- *Privacy and safety tools.* Most social networking services provide privacy and safety tools to enable users to manage 'who sees what' and whom they interact with on the service. These tools include a '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 which are 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 webpage/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

¹⁰The Children's Online Privacy Protection Act 1998 aims to protect children's personal information, including only allowing users over 13 years of age to register for a service without parental consent. In the UK the Data Protection Act 1998 requires organisations which process information relating to living, identifiable individuals to comply with its provisions and the act makes no distinction based upon age.

¹¹In the UK this is the British Code of Advertising, Sales, Promotion and Direct Marketing. www.cap.org.uk



on many social networking services sites, usually by clicking on a safety link at the bottom of every page.¹² Some social networking services provide online safety tutorials available on the site.

- *Moderation.* Moderation is an activity or process whereby a person and/or technical filters are responsible for reviewing content posted by users.¹³ 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 pose a challenge to social networking and interactive services where a considerable amount of content, including images, video footage and messages, are generated and uploaded by millions of users 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 provides 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. This could 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 is able to 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 comments from friends and a user can set their privacy setting to pre-moderate these comments before they appear on the page/profile.

What is social media?

Businesses, advertising companies, charities and also governments have recognised the potential appeal of user interactive services to reach global audiences and engage with supporters. This is commonly referred to as social media.

Specialist social media companies help brands analyse the market, optimise your audience, keep your content online fresh and moderate your webpage/ 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.

¹²The 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.

¹³Ref: Home Office Task Force on Child Protection on the Internet: Good practice guidance for the moderation on interactive services for children. 2005



Appendix B:

Sources of Safety Advice and Information:

The provision of safety advice to users of social networking services is recognised as critical. Government, law enforcement, children's charities and the industry on both an individual and collective basis have developed a range of safety materials to encourage safe and responsible use of the internet. Most of the resources have been developed to be shared and disseminated widely – and in some cases downloadable from the websites.

Child Exploitation and Online Protection Centre (CEOP): www.ceop.gov.uk and for safety and education materials www.thinkuknow.co.uk

CEOP is a police organisation focused on the protection of children and young people from sexual abuse and exploitation; it has a broad remit and range of functions to help tackle the sexual abuse and exploitation of children – primarily where use of technology is a factor, or media such as the online environment are utilised. It is also a founder member of the Virtual Global Taskforce (VGT), an international collaboration of law enforcement agencies committed to tackling this abuse of children and young people.

Through its holistic approach, CEOP aims to learn from its work and that of others to ensure that measures are put in place to prevent or reduce harm to children and young people in the future; this includes the development and rollout of an education programme called Thinkuknow for professionals to use with children and young people to help keep them safe online.

CEOP provides an online facility, in association with the VGT, for the public reporting of any sexually inappropriate or potentially illegal online activity towards a child or young person. For example, this might be an online conversation with someone who a child thinks may be an adult and who is engaging with that child in a way which makes them feel sexually uncomfortable, or exposing them to illegal or pornographic material, or who is 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.

Childnet International: www.childnet-int.org

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.

ChildLine: www.childline.org.uk

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.

Data Protection and the Information Commission Office: www.ico.gov.uk

'Keeping your personal information personal' – a guide to the Data Protection Act 1998 for Youth, including use of social networking.

Also has guidance on the protecting children's personal information for organisations

Good practice guidance:

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.

Website: www.police.homeoffice.gov.uk/operational-policing



- 14 -

Online behavioural advertising guidelines – Internet Advertising Bureau

Website: www.iabuk.net

CPSU Briefing on Photographs and Images of Children

Website:

http://www.nspcc.org.uk/Inform/cpsu/resources/briefings/PhotographsAndImagesOfChildren_wdf60645.pdf

Cyberbullying, a whole-school community issue - DCFS

Website www.teachernet.gov.uk

Internet Watch Foundation: www.iwf.org.uk

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.

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

Teachtoday : www.teachtoday.eu

Teachtoday provides resources for teachers on the responsible and safe use of new and existing communications technologies. Driven by Europe's leading internet, mobile network and social networking providers, working in partnership with European Schoolnet Teachtoday 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.

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

(April 2011)

