Dudley Safeguarding Children Board
Dudley Safeguarding Vulnerable Adults Board

Social networking services & social media:

Guidelines for safeguarding children, young people and vulnerable adults 2011

Dudley Metropolitan Borough Council

Dudley Children's Trust

Dudley Safeguarding Children Board

Contents

Acknowledgements

NSPCC Child Protection in Sport Unit Briefings
Social Networking services, social media and sport: Guidelines for safeguarding children and young people

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

1. Introduction

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

However, the use of social networking sites also introduces a range of potential safeguarding risks to children, young people and vulnerable adults.

As 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.

Both Dudley Safeguarding Board's guidance aims to help organisations consider the safeguarding of children, young people and vulnerable adults when using social networking sites.

It is recognised that when working with vulnerable adults, their capacity to make specific decisions must be taken into consideration when applying these guidelines. This will ensure that vulnerable adults are able to exercise choice and freedom whilst being encouraged to make decisions which promote their safety.

We want to provide information, advice and guidance on social networking services and other user interactive services to enable 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 including:**
    - **finding out more about the safety tools provided by social networking service providers and their acceptable use policies**
    - **taking the appropriate steps to safeguard the organisation's profile and its supporters online, in particular children, young people and vulnerable adults**
    - **promoting safe and responsible use by supporters of an organisation**
    - **assisting 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 on the Internet[1]. 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.

2. Who is the guidance for?

The guidelines have been developed for organisations considering the use of social media particularly:

- **people responsible for promoting opportunities to children, young people and vulnerable adults**
- **people with designated responsibility for safeguarding children, young people and vulnerable adults**
- **communications and marketing managers**
- **IT managers and webmasters**

They will need to work together to ensure the necessary safeguarding measures are in place and followed on a day to day basis. It is important your organisation takes ownership for safeguarding children, young people and vulnerable adults online and takes steps across the organisation to ensure safeguarding strategies, policies and procedures address online safety issues.

For member organisations of both Dudley Safeguarding Children Board and Dudley Safeguarding Vulnerable Adults Board this guidance should provide the framework for any safeguarding elements of internal policy and/or guidance.

3. What is social media?

Social media refers to the latest generation of interactive online services such as blogs, discussion forums, pod casts 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**

For more information on some of the common features that most social networking and interactive services have, refer to appendix 1 - Features of Social Networking Services.

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 people all over the world and share interests. Young people can design their own personal webpage, interact with friends through instant messaging and chat rooms, upload and share images and videos, create blogs, publish and share music and create or join wider communities or interest groups in areas such as music or sports etc.

4. The benefits of engaging with social media

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

- **promote the benefits of their services to all children, young people and vulnerable adults and it can be a route to the hard-to-reach groups too**
- **engage, connect and develop unique interaction with people in a creative and dynamic medium where users are active participants**
- **disseminate messages about events or campaigns virally among supporters in online communities**

It is important for organisations to give careful consideration to the use of social media and to balance the benefits of creativity, spontaneity and immediacy of the communication with the potential risks, including the risks to children, young people and vulnerable adults.

You should only move forward with developing social networking sites when safeguarding issues have been adequately assessed and addressed to minimise these potential risks.

5. What are the potential risks to children, young people and vulnerable adults 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, including self-harm, racism, hate and adult pornography[2].

Most children, young people and vulnerable adults 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:[3]

- **bullying by peers and people they consider 'friends'**
- **posting personal information that can identify and locate a child, young people and vulnerable adults offline**
- **sexual grooming, luring, exploitation and abuse contact with strangers**
- **exposure to inappropriate 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 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.**

6. Potential indicators of online grooming and sexual exploitation of children, young people and vulnerable adults

There is also concern the use of social networking services may increase the potential for sexual exploitation of children, young people and vulnerable adults. Exploitation can include exposure to harmful content (including adult pornography and illegal child abuse images), and encouragement for young people and vulnerable adults to post inappropriate content or images of themselves.

There has been a number of cases where adults have used social networking and user interactive services as a means of grooming children, young people and vulnerable adults for sexual abuse. Abusers use a range of techniques to make contact with and establish relationships with children, young people and vulnerable adults.

The Home Office Task Force on Child Protection on the Internet[4] 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**
- **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.**

Having made contact with a child, young person or vulnerable adult, abusers may also use that person as a means to contact and get to know their friends by using the links to their ‘friends’ in user profiles.

7. Good practice guidelines for organisations

The following guidelines contain practical safe measures for 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.**
- **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, young people and vulnerable adults online, sexual exploitation, online grooming and cyber bullying. 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, young people and vulnerable adults who interact with your webpage or profile. Ensure they understand online safeguarding issues, including warning signs of grooming and sexual exploitation and that they have an enhanced CRB check.

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 vulnerable adults before setting up your 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. (See appendix 1 - 'Features of social networking services')

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.

8. Setting up your social networking page

Use an official organisation email address

When you create a profile on a networking site such as Facebook, use an official 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 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 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 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 organisation.

Promote your social networking page on your website

Put the web address of your social networking web page/profile on your organisation's website. This will help users to find your social networking page and will reduce the risk of people finding fake profiles. Take care not to target or encourage potential users who are likely to be under the minimum age for the service. If you do not have an official social networking page state this on your website. This will ensure that users are aware that any other page using your organisations name is not an official one.

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

Once you have set up your 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.

9. Promoting safety online

Don't target underage children

When you're promoting your 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, young people and vulnerable adults

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

Be careful how you use images of children, young people or vulnerable adults

Photographs and videos of children, young people and vulnerable adults on websites can be used to identify them and make them vulnerable to people who wish to groom them for abuse. To counteract this risk, Dudley Safeguarding Children Board's use of images guidance must be considered before any images are used.

- consider using models or illustrations to promote an activity
- if a child is named, do not use their image
- if an image is used, do not name the child
- obtain parents' written consent to use photographs on web sites

Images showing children and young people under the age of 18 and vulnerable adults should not be used on any organisations social networking site e.g. FaceBook, flickr, twitter due to the potential for

- the tagging of children, young people and vulnerable adults thus identifying them at a location and allowing the opportunity for abusers to identify and locate them on social networking sites
- the morphing of the image
- personal intimidation by posting derogatory, abusive and threatening comments
- cyber bullying

There should not be the ability for users to upload their own images of children, young people or vulnerable adults on organisations websites or social networking sites.

For more details see the DSCB Use of Images Guidance.

It is recognised that some organisations may use campaign videos to raise awareness. Where such videos are produced organisations must:

- **gain explicit written parental consent for the use of video footage of children and young people under 18 on social networking sites (appendix 2)**
- **not allow comments to be made on the footage unless the comments are monitored by the media manager before they are posted**
- **use YouTube as opposed to Facebook to avoid the potential for tagging. Campaigns can be linked to facebook from YouTube**
- **not allow the capacity to 'share' the footage on facebook**

Such measures will help to eliminate the risk of children, young people and vulnerable adults being identified in footage, prevent unwanted comments being posted and prevent the footage being shared beyond the permissions gained.

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.

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. There are real challenges in managing a mix of organisation related content and other personal information, images and views posted by young people linked as 'friends' to the 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 written permission of young people and their parents and vulnerable adults and their appropriate carer before adding photos of or information about them to your web page/profile.

Promote safe and responsible social networking

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

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 web page/profile in the 'Friends' section.

Data Protection considerations

Take care when advertising events and competitions online when you are collecting personal information about users, including children, young people and vulnerable adults. 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 or 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, young people and vulnerable adults 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.

10. Safeguarding yourself - personal use of social networking sites

Due to the increasing personal use of social networking sites, employees and volunteers within the workforce should be aware of the impact of their personal use upon their professional standing.

In practice anything posted on the internet will be there forever and is no longer in your control. Remember when something is on the internet even if you remove it, it may have already been "snapshotted" by a "web crawler" and so will always be there. Current and future employers and service users may see this. Keep all professional work completely separate from your private life.

The following, in additon to the above, will help safeguard staff from allegations and protect employee's privacy as well as safeguard vulnerable groups.

Failure to comply with the following may result in organisations taking disciplinary action.

- social networking sites such as facebook have a range of privacy settings which are often set up to expose your details to anyone. When 'open' anyone can find you from a search of the social networking site or even from a google search. Therefore, it is important to change your setting to 'just friends' so that your details, comments, photographs can only be seen your invited friends. However, always remember anyone who can access your site can potentially copy and paste your comment into the public domain making it visible to all
- have a neutral picture of yourself as your profile image
- do not post embarrassing material or comments that may call into question your employment status
- do not accept friendship requests on social networking or messaging sites from students, pupils, young people (or their parents) or vulnerable adult service users that you work with. For those working with young people remember that ex pupils may still have friends that you may have contact with through your work with the organsation
- do not accept friendship requests unless you know the person or want to accept them - be prepared that you may be bombarded with friendship requests from people you do not know
- choose your social networking friends carefully and ask about their privacy controls
- exercise caution, for example, on facebook if you write on a friends "wall" all of their friends can see your comment even if they are not your friend
- there is a separate privacy setting for facebook groups and networks. You may have your own profile set to private, however, when joining a group or a network please be aware that everyone in that group or network are able to see your profile
- if you have younger friends or family members on your social networking groups who are friends with students, pupils, young people (or their parents) or service users that you work with, be aware that posts that you write will be visible to them
- do not use your personal profile in any way for official business. If you are going to be a friend of your organisations official social networking group ensure you have a seperate professional profile and do not use your personal profile
- do not use your work contact details (email or telephone) as part of your personal profile;

Tagging

You should always be aware of the privacy settings on photo sharing websites. If you or a friend are tagged in an online photo album (facebook, flickr) the whole photo album may be visible to their friends, your friends and anyone else tagged in the photo album. You do not have to be friends with anyone to be tagged in their photo album, if you are tagged in a photo you can remove the tag but not the photo.

Your friends may take and post photos that you may not be happy about. You need to speak to them first to request that it is removed rather than contacting the web provider. When over the age of 18 the website will only look into issues that contravene their terms and conditions.

11. Report safeguarding concerns

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, young person or vulnerable adult may be in immediate danger, always dial 999 for police assistance.

For further information on how to report concerns refer to Dudley Safeguarding Children Board procedures http://safeguardingchildren.dudley.gov.uk

The procedures also include guidance on safer working practices, management of allegations and the use of new technologies.

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 'Features of social networking appendix.

12. Social media, the law and good practice guidance

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

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. See appendix 3 for engaging with a social network service provider.

When contracting or outsourcing this work to a digital agency 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. See appendix 4 for information on working with a digital agency.

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 Data Protection Act 1998

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, young people and vulnerable adults. However, in the note on 'Collecting personal information using web sites' , the Information Commissioner makes the following comments:

- **web sites 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 (however Dudley Safeguarding Children Board guidelines recommend written parental consent for under 18s)**

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 web sites 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 web sites prohibit children under 13 from registering or using their sites.

Appendix 1

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 social networking services are US based where the law designates the age of 13 to protect children's privacy online, including their personal information. US law covers companies providing services in the US and overseas[5].

- commercial advertising. Commercial advertising may appear on various parts of the website. 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. 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.

- 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[6]. 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[7]. 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 web page / profile. A user's web page / 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.

Appendix 2

Consent form

Consent form for the use of video by (name of organisation)

Dudley Safeguarding Children Board and Dudley Children's Trust recognise the need to ensure the welfare and safety of all children and young people.

In accordance with Dudley Safeguarding Children Board and Dudley Children's Trust guidelines, photographs, videos or other images of children and young people will not be taken without the consent of the parents or carer.

Legal requirement In order to comply with the Data Protection Act 1998 a lawful basis is required before capturing images of a child or young person. Obtaining consent from either the parent, guardian or legally appointed representive of the child or young person provides that lawful basis.

Please tick relevant boxes I do ☐ I do not ☐ give consent for image capturing by video of

(insert child's name). . . . . .

For the purpose of : (Name of campaign and intended use for example PARKLIFE CAMPAIGN - VIA YOUTUBE AND FACEBOOK)

Print name . . . . . Relationship . . . . . .

Signature: . . . . . Date: . . . . . .

Contact telephone number: . . . . . .

Dudley Safeguarding Children Board and Dudley Children's Trust will take all steps to ensure these images are used solely for the purposes they are intended. If you become aware that these images are being used inappropriately contact your local social care team to report these concerns or visit http://safeguardingchildren.dudley.gov.uk/what-to-do-if

Consent is assumed indefinite, however, you do have the right to withdraw consent at any time. To withdraw consent please contact the marketing & communications team on 01384 815228.

Dudley Children's Trust

Appendix 3

Engaging with a social networking service provider

Make sure the service provider follows legislation and good practice

When you engage with 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 appendix 3 - 'Sources of information'.

Appendix 4

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 web page/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 at enhanced level**

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.

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, young people and vulnerable adults 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.

Appendix 5

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'.
www.dcsf.cov.uk/bvronreview/

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.org.uk

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 Child Line 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 web sites' 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.
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/poublications/operational-policing/social-networking-guidance/

Guidance for the Moderation of Interactive Services for Children
http://police.homeoffice.aov.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

Cyberbullying

The Teachernet site has a wealth of information on cyberbullying.
www.teachernet.aov.uk/wholeschool/behaviour/tacklinabullvina/cvberbullvina/

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.ora.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.teachtodav.eu

Footnotes

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 en1brcement, children's agencies and the internet industry, who are all working to ensure that children can use the internet in safely http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidancel

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

3. 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

4. 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 LD03

5. In the UK this is the British Code of Advertising, Sales, Promotion and Direct Marketing

6. 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 by young users

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

Useful contacts

For further information please contact;

Dudley Safeguarding Children Board
http://safeguardingchildren.dudley.gov.uk
01384 813061

Dudley Safeguarding Vulnerable Adults Board
01384 815870

Dudley Council's
marketing & communications team
01384 815228

Dudley Children's Trust
www.dudleychildrenstrust.org.uk