Derby City and Neighbourhood Partnerships

Derby City and Neighbourhood Partnerships

Social Media Guidance for Engagement with Children and Young People

Version control and document history

Document owner/author/manager	Adele Styles
Date of document	April 2014
Version	8
Document classification	Internal/External
Document distribution	Internal/External
Document retention period	Until date of next review
Location	Derby City Council Website
Review date of document	April 2017

If you require this document in large print, on audio tape, computer disc or in Braille please contact the document manager.

Contents

1. Introduction

1.1 Derby City Neighbourhood Partnership expects all members who engage with children and young people (CYP) should apply the same standards of practice both offline and online and work to clear guidelines and policies.

1.2 There are many benefits to using social media however there are also risks to CYP and organisational reputation. These risks can be managed to acceptable levels provided employees are aware of these risks and act responsibly.

1.3 Planned use of social media can be an effective method when engaging CYP in decision making.

2. Planning to engage children and young people online

2.1 If you are thinking about using social media or are already using it and want to review your practice, this may help you to be clear about your aims and objectives.

2.2 It is also important to research what is already happening in your local community in terms of social media and to get up to date with current trends and popular sites and services available.

2.3 Not all social media sites are appropriate. The site(s) that are used should depend on the objectives and what is to be achieved. It may be that a combination of sites is necessary.

Points to Consider	
Aims and Objectives	• What do you want to achieve? • How will you resource social media activities?
Policies and Procedures	• Ensure the social media policy cross references with other policies and procedures. For example code of conduct, safeguarding, communications, IT and network, internet and email user policy.
Confidentiality and Safeguarding	• Have safeguarding procedures in place • Identify the risks • Have a procedure to deal with cyber bullying, making a disclosure, online grooming and sexual exploitation.
Content	• The content needs to engaging, informal, two way and concise. • Be clear about timescales when responding to queries from users.
Legal Issues	• Have a disclaimer that states when and how you will moderate posts by users. • Identify a moderator and moderate daily. • Always seek consent before uploading images or content of individuals or groups.

3. How to get started

3.1 It is important that all organisations and that are using social media are aware of how to use each site properly, securely and that it is more than one person's responsibility.

3.2 All organisations and employers who are using and monitoring social media should be clear of their aims and objectives.

3.3 Access and Technology

Any new social media sites will need to be agreed by the management structure within the organisation. Any restrictions to access will need to be removed by the relevant employers.

Explore the possibilities of additional technology to help moderate the social media sites including mobile devices and additional software such as 'TweetDeck' which enables the management of multiple sites. There are many examples some are free and some cost.

In addition small organisation may only have one computer so therefore having individual log in accounts is strongly recommended.

3.4 Passwords and Accounts

The employers responsible for managing and monitoring the sites should set appropriate privacy levels and a secure password management system.

As privacy settings, terms and condition should change on a regular basis, it is important to keep up to date and review settings as necessary.

It is good practice to change passwords on a regular basis and choosing a password that is not easily identifiable. This includes 8 characters or longer, upper and lower case, number and symbols such as SP1D3Rm@n (Spiderman).

3.5 Disclaimer

A disclaimer is a good way to inform users about when, who and how the account will be managed and monitored including actions for potential libellous, disruptive, abusive or otherwise offensive posts.

The disclaimer should also where possible provide contact details of the organisation as well as emergency or out of hour's guidance.

3.6 Confidentiality

Do not publish information that may identify individuals and/or groups without their consent. Also do not publish information or decisions from within an organisation without prior consent.

An example of this could be publishing consultation results where the information provided can identify an individual or group and/or the information about the decision by the organisation is politically or commercially sensitive.

3.7 Personal Conduct and Responsibilities

The social media sites should be in the name of the organisation rather than individual members of employees.

An organisations code of conduct for employees should cover both professional and private online behaviour. For example, employees must not bring the organisation into disrepute by either their personal or professional offline or online behaviour.

Employees must not cross professional boundaries by having CYP as 'friends' on their personal social media sites. CYP may actively try to search for employees' personal social media profiles. Employees should check privacy settings to prevent access to personal and sensitive information. There is a very real risk of the ability to duplicate a profile and pose as someone else.

Employees should act as good role models in their use of social media and educate CYP to be responsible and safe.

4. Content

4.1 When making a decision about the content, the following needs to be considered:

- Plain English
- No foul language or slang
- Proof read by an independent person
- CYP friendly
- Varied and interesting
- Interactive/responsive
- Not leading or persuasive
- Regularly updated
- Represent the organisation

4.2 Remember social media is about interaction so if the organisation plans to simply post information and news one way it may actually disengage CYP in the process.

4.3 Consultation

Involve CYP in the design and development of social media channels as appropriate.

Social media can facilitate opinion polls, online surveys, discussion boards, open interaction and conversations, providing information and sign posting. Be aware that some forms of open communication will need moderating and this requires resource and time.

However as with any other form of consultation, the format must not have leading questions or statements and should use both qualitative and quantitative methods.

Please refer to the Derby City and Neighbourhood Partnership Participation Standards for best practice.

5. Safeguarding

5.1 Ensure safeguarding policies cover the potential risk to CYP online, such as grooming, sexual exploitation, sexting and cyber bullying.

5.2 If an organisations social media account is open to public comments then the organisation has a responsibility to respond to any issues or concerns raised by CYP, parent/carers. There must be a procedure in place.

5.3 Helping CYP to protect their privacy online

Most social network providers have settings for user protection, including privacy tools. There are some simple, practical measures CYP can put in place to reduce risks when online. Here is some guidance to help CYP stay safe online:

- Explain the importance of privacy settings and advise how to put them on, note location privacy by keeping apps and programmes off unless needed such as blue tooth and GPS settings.
- Explain that only people that they allow should be able to see what they post and comment on their space, rather than public.
- Explain importance of password or pin protecting online devices recommending a password which includes a mix of capitals, numbers and symbols.
- Advise not to publish personal information that would identify a child such as; images of family and friends, phone numbers, school, meeting places, home and email address and BBM pin.
- Advise that once information is published online it will always be accessible to everyone even after they have removed from their page.
- Advise not to accept friend requests from people that they do not know including friends of a friend.
- Advise never to meet people off the internet and to tell a trusted adult if someone has asked them to.
- Discuss the potential risks of accessing adult social networking sites and websites.

When CYP interact with the organisations social network accounts it may be possible to ‘test’ how secure or private they are by clicking through various parts of their profiles to see what’s publicly visible. This could then be fed back to the individual highlighting the risks and advise them to set their privacy settings.

5.4 Concerns about Grooming

Child grooming is a process used by people attempting to form a relationship with CYP by pretending to be their friend and to prepare the child for sexual abuse. This can take place through social networking, gaming sites and private messaging. Once a relationship is established the communication may become graphic, requests for images, web cam use or plans to meet the child in person can occur.

If you have concerns that a child or young person is being groomed over the internet you must follow the Derby and Derbyshire safeguarding procedures: http://www.derbyscb.org.uk/

For further support contact Safe and Sound Derby to discuss any concerns and for guidance on how to progress.

5.5 Cyber Bullying

Cyber bullying is the use of technology to bully a peer or child, this can occur via text messages, emails, posts on social networking sites, posting of embarrassing pictures, videos or fake profiles.

Most social media platforms have their own reporting mechanism for cyber bullying which allow CYP to report their concerns directly. Read more at www.stopbullying.gov All professionals should also familiarise themselves with CEOP and Think You Know.

CYP should also be provided with guidance about what to do in these circumstances and if you become aware that a child is experiencing cyber bulling ensure to follow safeguarding procedures of your organisation.

6. Legal Issues

6.1 Employers and employees will be held legally responsible for content published online.

6.2 Making a written statement (on or offline) about a person or company that is considered to harm reputation is known as libel and legal action will be taken against the organisation and/or employee. This also applies to both personal and work related accounts, in and out of office hours.

6.3 Before posting information or images, music or videos onto social media sites it's important to make sure you have permission, making sure you follow the legal framework of Data Protection and Copyright.

6.4 When publishing images or videos of CYP, always get signed permission from the young person and parent/carer.

6.5 It is good practice to never mention work, opinions of colleagues, projects or processes on your own social media networks. Where promoting a public event or project; seek guidance from your employer before posting information.

7. Training

7.1 Investing in social media training for employees is essential to:

- learn good practice/new channels/ideas
- ensure the organisation is using social media appropriately and safely
- minimise risks.