DIOCESE OF
DOWN & CONNOR

Addendum 3:
Guidance on Using Social Networking Services and Social Media: Promoting Safe and Responsible Use

BEST PRACTICE IN SAFEGUARDING AND
PROTECTING CHILDREN AND YOUNG PEOPLE
AND THE ADULTS WHO WORK WITH THEM

GUIDANCE ON USING SOCIAL NETWORKING SERVICES AND SOCIAL MEDIA: PROMOTING SAFE AND RESPONSIBLE USE

Purpose of this guidance

This guidance has been produced to provide comprehensive information, advice and guidance on social networking services and other user interactive services to enable Diocesan groups/ bodies, parish groups and Youth Centres 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 as a means to:

- 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 parish and its staff, volunteers online, in
- particular children and young people;
- promote safe and responsible use by parish staff, volunteers and children and young people;
- assist those organisations with an existing presence on user interactive services to develop, review or update their policies and practice guidance.

Pope Benedict XVI, in his message for 44th World Communications Day, chose as his theme: *The priest and pastoral ministry in a digital world: new media at the service of the Word.*
He states, “Using new communication technologies, priests can introduce people to the life of the Church and help our contemporaries to discover the face of Christ. They will best achieve this aim if they learn, from the time of their formation, how to use these technologies in a competent and appropriate way...” (CiNews, 27/01/10)

This guidance reflects the current good practice guidance produced by the Home Office Task Force on Child Protection on the Internet. 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 guidance will be useful for all those involved in parish groups considering the use of social media. It is important that your parish takes ownership for safeguarding children and young people online and takes steps across the Diocese to ensure safeguarding strategies, policies and procedures address online safety issues. This guidance specifically targets the following people in the Diocese and your parish:

- The Director for Safeguarding /Designated Officer responsible for promoting and ensuring the safety of children and young people
- Designated persons responsible for safeguarding children
- Child Care Committees
- Parish Group Leaders
- Senior Youth Centre workers
- Diocesan Media and web controller

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?

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. Social media provides unique opportunities for Diocesan bodies and parish groups to engage with, connect and develop unique relationships with people in a creative and dynamic medium where users are active participants. Information about parish activities and messages can be disseminated widely amongst supporters within online communities.

Most young people, and many adults, are actively using the wide variety of the social networking websites. Some examples of popular services include: Bebo, Facebook, Flickr, Piczo, Hi5, MySpace and Twitter. Other services focus on video sharing and include Youtube.

It is important for Diocesan bodies and parishes to give careful consideration to the use of social network sites and balance the benefits of creativity, spontaneity and immediacy of the communication with the potential risks, including the risks to children. (See point 4 below)

Your parish groups 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, including self-harm, racist, hate and adult pornography.

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

- 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 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/ girlfriend?’ 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 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. Nevertheless it is important that Diocesan and parish groups are alert to these indicators as this will enable appropriate preventative action to be taken.

Good Practice Guidelines for the Safe Use of Social Media

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

If your parish group/Youth Centre 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 the steps you should follow at this stage are to:

- Assess your needs and readiness
- Consider what your objectives for use are eg. interaction with users, publishing, or a mix of both
- Consider the medium that you want to use.

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

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 parish group's/ Youth Centre's 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: What is social networking and social media?

2. **Your Diocese/ parish should follow relevant legislation and good practice guidance when engaging with social media companies**

Depending upon the size of your parish group/ Youth Centre, 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 Bureau5)
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 C:

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

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

3. 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.
- Collection and use of personal data and the Data Protection Act 1998.
- Access NI checks where moderators are used on services likely to attract children in accordance with the Safeguarding Vulnerable Groups Northern Ireland Order 2007.

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 Access NI 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 by:

- **Ensuring that the Parish/ Youth Centre webpage/profile adheres to existing good practice policies** including safeguarding and child protection, privacy of personal information, the use of photographs and acceptable behaviour.

- **Reviewing 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 cyber bullying. Remember that personal and group disputes can easily overspill 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 Diocese's Designated Officer, 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.
  In the UK, illegal sexual child abuse images should be reported to the Internet Watch Foundation at www.iwf.org
  Reports about suspicious behaviour towards children and young people in an online environment should be made to the Child Exploitation and Online Protection Centre at www.ceop.uk.

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

- **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.

5. Decide how your webpage / profile will be managed within your parish group / Youth Centre

- **Management of the profile**

Decide who will have responsibility for: the setting up; management; and moderation (overseeing/reviewing/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.

- **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.

- **Involve your Designated Officer**

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

6. Registration or ‘signing up’ your parish group/ Youth Centre:

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

This requires an email address – use an official parish/ Youth Centre email address rather than a personal email address. This will reduce the risk of the establishment of imposter 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 diocesan/ parish 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 parish /Youth Centre. This will reduce the risk of the activity 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 parish and/or the Youth Centre, and require the intervention of the

Diocese, the service providers and the National Safeguarding Office 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 Group leader / Diocesan Designated Officer)
The Safeguarding Vulnerable Groups (Northern Ireland) Order 2007 includes moderators who have responsibility for interactive services.

- **'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 parish group/ Youth Centre 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 are aware of the need to protect their privacy online**

Make sure that your staff (paid and volunteers), children 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 damage their reputation before they link their webpage/profile to the parish group/ Youth Centre profile.

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

- **Parish Group/ Youth Centre details**

Add information about how to contact your group/ Youth Centre leaders including a website address, if available. Also include offline contact details for your club and any information on membership of a Youth Centre parish group.
.

- **Promote your parish/ Youth Centre webpage/profile**

Feature details of your organisation's social networking webpage/profile on your 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 parish / Youth Centre webpage / profile.

- **Promote safe and responsible use**

Consider promoting safe and responsible use of social networking to all children and young people who access parish related activities and/ or Youth Centres online. If you do not yet have a safe and responsible use policy or safety tips for your parish group/ Youth Centre, there is a considerable amount of safety material available.

- **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 parish/ Youth Centre webpage/profile in the ‘Friends’ section.

- **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 any parish/ Youth Centre event and signpost to where users can obtain further information e.g. further information can be obtained from your the group leader or on the club notice board etc.

- **Uploading Content – ‘think before you post’**

Consider any messages, photos, videos or information – do they comply with existing policies within the Diocese /parish? 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 parish/ Youth Centre webpage/ 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.

(Adapted from NSPCC Guidance on Social Networking and Social media use)

January 2012

This policy and guidance is in keeping with *Standard 3- Preventing harm to children, Standards and Guidance Document for the Catholic Church in Ireland (Jan 2009)*