Guidance

Keeping Children Safe

Keeping Children Safe Online

A guide for organisations

We have made every effort to take into account best practice in the preparation of this document. However e-safety issues can be complex and have the potential to be multi faceted. This advice does not constitute legal advice and the authors and contributors can therefore accept no liability for any damage or loss suffered or incurred whether directly, consequently, indirectly or otherwise by anyone relying on the information in this publication or any other information referred to in it.

URLs and references given in this document were correct at the time of publication but may be subject to change over time.

Authors and contributors

This guide has been developed by Charlotte Aynsley for Keeping Children Safe in consultation with key international NGOs (Plan International, World Vision, War Child Holland and Save the Children).

Acknowledgements

Charlotte Aynsley and Keeping Children Safe would also like to thank the Child Exploitation and Online Protection Centre (CEOP) for their help and support. Thank you to the Oak Foundation, Save the Children and Plan International for their financial support.

Please note

For the purposes of this guide:

E-safety: keeping children safe in the electronic world

ICT/ICTs: information communication technology, that is technologies that provide access to information through telecommunications. These include the internet, wireless networks, mobile phones and other communication tools

Social media: a way of interacting amongst people in the virtual world. It includes social networking, weblogs, social blogs, microblogging, wikis, podcasts, photographs, videos and pictures. In this guide the main focus is communication through social networking though other platforms are considered.

Contents

Introduction

This guide is based on a model that helps organisations plan their approach to the use of social media. It also signposts sources of further support: advice, training and information.

What does the guide cover?

The guide has been developed for international NGOs who want to use social media with children and young people that they work with. They may want to develop children's skills and capacity; to use social media as a development tool for a community project; to provide access to technology; or to offer social media as a communication tool between communities or between sponsors and sponsored children.

The advice is targeted particularly at NGOs working with children and young people in developing countries where there is an increasing use of social media and a need for organisations working with children to protect them in the online world.

In today's increasingly digital world, the issue of e-safety, that is keeping children safe in the electronic world, is extremely important.

Why is it important to provide advice in this area?

NGOs are increasingly engaging in projects or activities that use social media as a form of engagement, empowerment and development. This can vary from internet radio through to Facebook or Twitter as well as the use of ICT for development projects to advance human rights or social and economic well-being.

ICT has huge benefits for children and young people: it provides access to a range of often inaccessible resources, communication and support. However, social media also creates potential risks for children.

It is essential therefore that organisations, which are planning projects, have guidance and support to protect children and young people, manage risks and maintain the highest levels of child safeguarding standards.

Using ICT positively: Conflict in South Sudan and Uganda means there is a serious lack of employment opportunities for young people. Many have never received an education. War Child Holland has worked with communities to set up independent youth organisations to improve opportunities for children and young people. They have set up fully youth-led, independent and easily accessible ICT and Resource Centres, providing children and young people with a safe environment where they can develop essential life and ICT skills, engage in children's rights promotion and learn to express themselves freely using media and ICT. In one centre in Uganda the project has generated employment opportunities and most of the young people involved have gone back to school. Reports also show there has been a reduction in fights, criminality and use of alcohol in the regions where centres have been established. Source: Building self-sustaining ICT and resource centres, War Child Holland, 2014

Overview of risks

British psychologist Dr Tanya Byron highlighted the risks posed to children and young people online in her review of children in the online world in 2008. As part of the review the London School of Economics categorised the risks as the 'three Cs': content; contact; and conduct. They give a framework for considering risks posed to and by children online.

	Commercial	Aggressive	Sexual	Values
Content – child as recipient	Adverts Spam Sponsorship Personal information	Violent/ hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading information or advice
Contact – child as participant	Tracking Harvesting Personal information	Being bullied Being harassed Being stalked	Meeting strangers Being groomed	Self harm Unwelcome persuasions
Conduct – child as actor	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading information or advice

Source: The Byron Review – Safer Children in a Digital World 2008. Developed by the EU Kids Online Project

Content: refers to material that children and young people can access online: commercial (adverts or spam); violent or hateful material; pornographic or sexual material, and racist or biased content. The principle of the "Content" risk is that children access and come across online material as passive recipients. This may expose them to risk.

Contact: refers to children and young people as participants – they are actively involved in the interaction. They may share information about themselves, which puts them at risk. Their information may be harvested or tracked. They may be stalked or bullied; meet strangers on and offline, or be subjected to grooming.

Conduct: involves children or young people engaging in risky behaviour. They may download something illegally, bully or harass another young person or adult, create and upload sexual material or 'sext'.

Further risks were identified in a report compiled by the Berkman Center for Internet & Society at Harvard in collaboration with UNICEF, which was published in 2010. Evidence suggested that risks for children in the developing world have a different focus to those in the industrialised/developing world. The following areas were highlighted:

- In Indonesia and the Philippines there is evidence that new forms of producing and distributing pornographic materials are taking place in internet cafés, where broadband connections at home are still low. Private booths in internet cafés are equipped with PCs and webcams which are then used by girls for online striptease shows in return for money transferred to their prepaid mobile phone accounts.

I learnt about the internet and how to use it from an organisation that worked in my town for a while. I then started using an internet café every week to speak to my friends and my relatives abroad using the internet. I got really friendly with the owner and he used to help me if I ever had any technical queries or questions. He asked me to come into the back one day and said he had friends online who wanted to talk to people. At first chatting to his friends online was fun. They seemed really interested in my life and interests. They asked me to turn on the camera on the computer and then told me that I was very pretty. They asked me if I'd like to make some money – lots of girls were making money and all they had to do was take their tops off whilst chatting – it was harmless. When I first did it and got paid, I was really pleased because me and my family needed the money but it soon escalated and I was doing more and more stuff but the money went up as I got more and more daring so I carried on. 15 year old – Philippines

- **Sexting:** Teenagers are using mobile phones to produce clips featuring boys and girls engaged in sexually explicit behaviour, highlighting the role of mobile phones in the distribution of such materials in the developing world. Sexting is also an increasing phenomenon in India and South Africa, using MXit (a popular instant messaging service). Increasingly photos were reinforcing offline gender based relationships; that is photos were used as "currency" and status.

- **Grooming:** There is still limited data on grooming by adults or peers via social networking sites or interactive platforms but surveys from Thailand indicate that 24% of responding children met with someone offline they first met over the internet and in 58% of these cases the meeting turned into an unpleasant experience because their virtual friends had lied. Older children (25% of respondents) indicated that correspondents have invited them to engage in sexual activities. A qualitative African study highlighted that a popular IM service is used to distribute pornography and allows pedophiles to contact minors by pretending to be minors themselves.
- **Cyberbullying:** is probably the biggest risk that children and young people face in the developed world but it is also on the rise in countries such as China, South Africa, India and Thailand. A study in India suggests that 65% of surveyed school students have been victims of mobile phone bullying and that 60% have been involved in bullying others.

Data from Thailand indicates that 35% of seven-11 year olds have had exposure to web sites displaying pornographic material. Of older respondents 71% have visited porn sites voluntarily. A report from the Philippines indicates a link between the rise of internet cafés and increasing access to pornographic sites. This was also found to be the case in Dakar in Senegal.

A particularly serious risk that has been identified in developing countries is exploitation of young people via social media from donors, especially where there is a one-to-one sponsorship arrangement. Keeping Children Safe has provided detailed guidance around best practice for managing communication using social media with donors and sponsor children. See Appendix 6.

Social media offers new opportunities for contact by donors and abuse can take place online – via web cam for example – and can also lead to offline abuse:

- Donors can make unsolicited contact via social media, tracing children and their families.
- Sponsored children can receive unwanted and inappropriate images/content.
- Sponsored children could experience live/real time abuse – particularly sexual abuse via social media.
- Children may be subjected to an increased network of adults who wish to exploit them.

At present there is little evidence that donors are abusing children and young people via social media but NGOs have recognised that where there is one-to-one sponsorship of a child there is an imbalance of power and therefore an opportunity for exploitation.

Social media provides new opportunities for tracking, identifying and abusing both on and offline. Organisations need to recognise and manage this risk effectively.

As technology evolves and access becomes more widespread the risks and issues will evolve and change. It is important always to understand the most pertinent risks in your context.

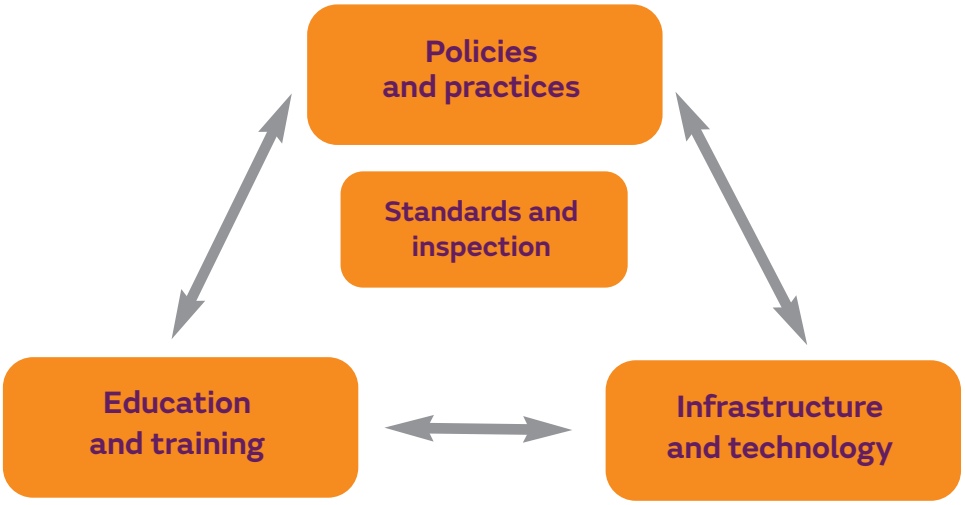
Social media provides new opportunities for tracking, identifying and abusing both on and offline. Organisations need to recognise and manage this risk effectively.

Using social media safely

The PIES model

When organisations are planning projects involving the use of social media and digital technology, they need to understand the environment in which they are working in order to reduce the risks to young people. The PIES model, which has been tried and tested in the UK and elsewhere, is an effective tool for reducing risks. (Becta, 2009)

The PIES model centres around four core areas: Policies and practices; Infrastructure; Education; and Standards.



Source: Becta, 2009

Policies and practices: refer to the types of e-safety policies and procedures that organisations need to have in place. For instance, a policy should describe the acceptable use of technology and outline the sanctions should this be breached.

Infrastructure: The technological infrastructure that an organisation uses plays a key role in protecting children and young people. Organisations need to consider which technical solutions can be implemented to ensure safety.

Education: Organisations must ensure that staff, volunteers, children and young people, as well as the wider community, receive the most appropriate education and training in the proper use of ICT and social media.

Standards: All the above need to be constantly monitored and reviewed in order to protect children and young people. Ongoing reviews of the 'standards' of the approach are essential and need to be carried out across different levels, including internal child safeguarding, social media standards or guidelines, external laws or governance arrangements, or inspection approaches.

Putting the PIES model into practice

The checklist below can be used to implement the PIES model:

1 **Understand the context and risks:** research the context in which your organisation will use social media and which legal instruments support safeguarding. Carry out an audit with key stakeholders to establish levels of use, risk and awareness. Use this to shape your approach.

2 **Policies and practices:** examine and assess existing policies such as child safeguarding, reporting, and escalation policies and processes. Consider whether existing policies cover the relevant aspects. If not, develop new policies, particularly relating to social media and acceptable use. Involve stakeholders to do this.

3 **Infrastructure and technology:** look at the most appropriate technology and/or services to use. Set up technical solutions that will help to lessen and manage risks to young people, staff and volunteers.

4 **Education and training:** consider educational approaches for all involved – staff, children and young people, volunteers and parents and carers.

5 **Standards:** use internal and external feedback to continually inform and develop the approach.

Expanding on the checklist:

1. Understand the context and risks

Research the context

When planning any project that incorporates social media, it is important to take into account the legal and cultural situation in the area where the project will take place. Local and international laws relating to online abuse must be followed in order to safeguard children and young people.

Key international conventions and protocols exist that include references to online abuse and set out standards which other countries should adopt. See Appendix 2. International legislation aims to create a framework of child rights and safeguards, which can include definitions of offences so allowing for more effective prosecution of perpetrators. Combined with local legislation, this should enable countries to develop ways of addressing child abuse and exploitation.

Online abuse is often a transnational crime — one that has no “borders”. Perpetrators may be located in different countries to their victims. Law enforcement agencies have a vital role to play in ensuring that laws are applied consistently and effectively and that offenders are prosecuted. However, levels of capacity, technical expertise and resources vary. Many countries do not have sufficient legislation to combat child abuse images, or criminalise grooming. This can make international incidents complex to manage. There is also a global lack of awareness among parents/carers and key child protection agencies about online behaviour and abuse, which may mean there is a lack of prevention and protection strategies in place to safeguard children. There is, therefore, a greater need for collaboration between law enforcement in different countries, taking into account different jurisdictional protocols and social, cultural and political issues.

Local cultural and social issues may affect risk, access and education. These need to be taken into account when planning strategy. Local laws too may affect the way in which e-safety strategies can be implemented.

Conduct a risk assessment

Every organisation will have slightly different policies and practices, technical infrastructure, education and training opportunities and standards. How these are applied and implemented will vary in relation to context. However it is important that e-safety is integrated into existing policies and practices.

Before planning projects using social media, it is advisable to carry out a risk assessment or audit in order to review and understand the safety risks within the context in which you are working. This needs to take place before implementing any social media strategy. The audit will help you understand the type of approach that needs to be taken and the issues that need to be tackled.

Questions to consider for audit:

- How and where is social media to be used?
- What kind of social media is going to be used?
- What are the favoured methods of online communication?
- What is the current state of play in relation to online safety education and training – for staff, children, parents, the wider community and volunteers?
- What is the attitude towards access and risk in the local community?
- What policies and procedures already exist for online and social media use?
- How can existing practices and policies be linked to online safeguarding issues?
- What reporting and escalation procedures exist for safeguarding risks to children? (In terms of escalation, if there is an issue which senior person manages and receives the report, and who is responsible for dealing with the issue?)
- What kind of online safety incidents have already arisen?
- What has been the outcome?
- What sorts of risks are children, parents, the community and staff worried about?
- What does your organisation need to address? What are the concerns?

An NGO that is working with children in the field will have a variety of policies and practices to ensure the safety of children and the protection of its staff and volunteers. Use Keeping Children Safe's other resources to check you have all child safeguarding standards in place.

www.keepingchildrensafe.org.uk/resources

2. Policies and practices

All policies – child safeguarding, sponsor and donor policies, communication and behaviour policies – must make reference to ICT/social media and other online interactions as well as offline interactions because of the high risks involved.

If you do not have any existing policies and you are using, or intend to use, social media as a communication tool, you need to develop a policy. Organisations that do not have policies of this type are putting themselves at risk. Do not instigate a new project using social media or technology without first having clear polices in place.

A social media policy

A social media policy is essential to set out how an organisation plans to develop and establish its approach to social media and to identify core protocols regarding safe conduct. The policy should describe the organisation's expectations regarding social media use, as well as explaining any sanctions for misuse (especially for staff). The policy should outline clearly how social media use will be managed and what is considered to be safe practice as well as how this will be communicated.

A social media policy will need to include:

- an introduction to social media and the context of use
- the legal framework – what laws may be applicable regarding use of social media within the respective context. This may depend on the use of social media concerned and may also need to consider local and international laws that might be involved
- cross-references to other related and existing policies on child protection and safeguarding, as well as guidelines and protocols
- information for children, young people and families regarding safe and positive conduct, as well as sources of support
- information about staff's personal use of social media and expectations of positive conduct as well as clear procedures to follow if there are concerns
- information about safe donor use of social media, including protection from fraud, scams and so on
- how internet use will be monitored (if appropriate)
- how concerns will be managed and what sanctions (where appropriate) may be used. This should spell out clearly what is considered illegal and unsafe behaviour
- clear information about the organisation's procedure for reporting and investigating concerns, including a named point of contact. Sources of support within the organisation and externally should be included
- the role of managers in implementing and supporting the policy
- how the policy will be communicated throughout the organisation, for instance via staff training and information (videos, literature, training) for children and donors
- how and when the policy will be reviewed and updated, ideally annually.

Organisations need to have clear guidance and procedures regarding the safe and appropriate use of social media for all stakeholders, including staff, children and young people and volunteers.

Organisations cannot ban staff, children or donors from using social media sites in their own personal time. However, they can, and should, put in place guidance and boundaries. They should use various approaches to embed safe practice and increase awareness regarding appropriate behaviour. Boundaries should explain clearly what is considered appropriate behaviour for staff and expectations around the use of social media in and out of work time. See Appendix 3 for a template social media policy.

Organisations which facilitate communications between children and donors need to ensure additional layers of safety to safeguard those children from potential risks posed by donors. See Appendix 6 for detailed advice.

Acceptable Use Policies (AUPs)

If you are providing access to social media as part of a project you **MUST** produce an acceptable use policy (AUP). This sets out an organisation's approach to online safety. Its aim is to protect children and young people, staff, volunteers and the wider community from online risks. It is a separate document from a social media policy and should be developed for a wide range of people – for instance staff, children and young people, parents/carers, donors and volunteers. It should complement and reinforce the organisation's social media policy.

Ideally an AUP should consist of two documents:

An overarching management/internal document: this highlights the organisation's vision and approach to social media, including acceptable and unacceptable use of technology, sanctions for misuse and the procedure and timeline for responding to, and reporting, misuse.

An end user document: this is an accessible explanation of the management/internal document and is aimed at users, including children and young people, staff or volunteers. The tone and approach need to be meaningful to the users so they should be included in developing an AUP.

> The children's charity Childnet International, part of the UK Safer Internet Centre, have developed a suite of materials for children and young people to help them to think about their rights and responsibilities online. Have a look at the materials **http://www.childnet.com/teachers-and-professionals**

See Appendix 7 for advice on helping children to develop healthy online communication.

An AUP assists the organisation by:

- setting out clear boundaries and providing clear expectations regarding the appropriate use of technology
- providing a clear and concise outline of what the organisation considers to be acceptable and unacceptable behaviours
- encouraging users to develop responsibility for their behaviour
- outlining monitoring procedures
- outlining sanctions concerning use
- signposting users to sources of support.

An AUP should contain core statements that users sign up to before and when using online technology. The AUP will describe how these are implemented.

Core statements should include the following:

- All users take responsibility for their own use of technologies making sure that they use technology responsibly, safely and legally.
- All users will receive e-safety training and education from the organisation.
- All users will sign up to the terms in this policy.
- No communication device will be used to bully, harass, intimidate or abuse another person.
- All users have a responsibility to report any known misuse of technology.
- All users have a responsibly to support fellow users.
- All users have a responsibility to protect their own private information including passwords. Any attempts to access, corrupt or destroy another persons information is unacceptable.
- All users should understand that access is monitored.
- All users should be aware that where access has been granted by the organisation we reserve the right to confiscate or investigate fully communications if we need to do so.
- Users will report and escalate issues to the respective contact in their local area especially if they have concerns over abuse by themselves or others.
- Users will use cameras and communication tools safely and responsibly and will not abuse, harass, embarrass others or themselves.

Source: Adapted from AUPs in Context: Establishing safe and responsible online behaviours. Becta 2009.

Code of conduct

Any social media policy and AUP must include a professional and personal code of conduct for staff and volunteers using social media. See guidelines below:

- Children's safety is of utmost importance.

- Professionals and volunteers working with children are in a position of trust and need to be responsible at all times, no matter what media they are using.
- Staff and volunteers also need to protect themselves online.
- Staff and volunteers are subject to scrutiny even if using social media in a personal capacity.
- Sanctions and codes of conduct are expected and should be adhered to.

See Appendix 5 for a sample code of conduct

Organisations should also draw up a protocol for staff and volunteers, which describes procedures that they should take when using social media.

Protocol for the use of social media:

- If you already use social networks or blogs for personal use and you have indicated in any way your place of work, you must add a disclaimer stating that opinions on this site are your own.
- If you want to start a social network or blog for reasons associated with your organisation, for instance to further participation, engagement and consultation, you must consult your manager and follow existing communications, child safeguarding and e-safety policies.
- You must produce a valid business case for using social media professionally.
- You need to describe your target audience and what you intend to communicate or learn.
- You should explain your aims for the social network or blog and why you think it is the right communication platform.
- You should advise which other channels of communication you will use to support your social networks.
- You should state how many times a day you intend to update/check the social network or blog and who will do this for you if you are sick or on leave.
- You must state how you will keep records of data that you post.
- You should describe your commitment to reviewing the social network or blog and providing your manager and the communications team with data to ensure it is being used effectively.
- You must review content regularly and describe how you will monitor, moderate and manage interactions.
- You should commit to stating clearly on the social network or blog when you leave the organisation and hand over the site to the person who comes into your post.
- You are personally responsible if you break the law, for instance by posting derogatory comments or inappropriate material.

3. Infrastructure and technology

All social media based projects must include technical solutions to protect children and young people from accessing inappropriate, harmful or abusive content. These should be included in the AUP so users know how their access is being managed.

The following e-safeguards should be put in place whether the organisation is providing internet access through a centre, or on a one-to-one basis:

- Anti virus software to prevent the spread of viruses through machines.
- A firewall to prevent unauthorised access.
- Filtering to allow only certain types of content to be made available. Two types are available: whitelist filtering lists acceptable sites and services; blacklist filtering blocks out websites and services.
- Personal profiles and preferences: these can be created for young people so that when they log on to their personal profile, it only allows access to appropriate content.
- Monitoring so that content that has been accessed can be flagged up. It can be reactive or proactive, that is content can be checked retrospectively or flagged and blocked when someone accesses the network.
- Controls to ensure that only appropriate content is accessed. Web cams or internet access can be switched off mobile phones. Safe searching can be set up on mobiles, PCs and laptops.

4. Education and Training

Ongoing education and training for staff, volunteers, young people, parents and donors is an essential element in achieving e-safety. All concerned need to be aware of e-safety and be trained in strategies to deal with risks that may arise. Training should be continually reviewed and updated to reflect the current situation, and should be adapted to suit the needs of users and the community. It can be delivered directly or through national or local awareness campaigns. Various NGOs, government organisations and charities offer e-safety training.

Education and training for staff

Education and training for staff is crucial at both a local and a national level. It should be ongoing and embedded within existing training programmes. It should cover new and emerging risks, child safeguarding and solutions.

- CEOP offer training internationally to practitioners who work with children www.ceop.police.uk/icpn.
- Unicef offer e-safety training – www.unicef.org.
- www.childnet.com have resources and support.
- www.thinkuknow.co.uk is CEOPs education programme for professionals.

Education and training for children and young people

Education and training for young people is crucial to limit risk. It can range from basic awareness to more in-depth higher level education. Organisations such as World Vision have developed e-safety information and support specifically aimed at children and young people.

World Vision has produced an interactive CD for children with cartoon characters explaining how to be safe online. The CD is is used for training and has been well received.

"This CD is wonderful and simple," says Mirgen Fejozlli, a teacher in Plasa village. "I am going to show it to my pupils, in elementary school. In the same time I can show it to the parents, during our meetings."

Leaflets, awareness videos, and posters were shared with partners, children and young people to show the potential risks of online abuse, such as pedophiles and online bullying. Resources include contact information for the National Helpline for children, Alo 116, where children can report incidents.

"We are happy to provide this knowledge and practical tools to children, parents and teachers in Albania, where online abuse is on the increase," says Mandy Yamanis, Child Protection Expert, World Vision."For Albania, online abuse and its consequences are a new phenomenon for which we have to be prepared to respond and support children when needed," says Ridiona Stana, the Child Protection Manager of World Vision in Albania and Kosovo.

As an example of the practical tools Yamanis reminded parents, "Never leave the computer in a child's room. Put it in the living space where you can monitor what he or she is doing. Talk to your children and encourage them to use their mobile phones wisely [and, most of all] make sure they understand that once a photo or personal data is put on the internet and is part of the world wide web, it can never be removed."

Source: http://wvi.org/albania/article/albania-children-learn-be-safe-online-1

CEOP also have information specifically for young people www.thinkuknow.co.uk. Childnet has further advice and support www.childnet.com.

Safer Internet Centres exist across Europe. You can find a full list at www.saferinternet.org.

Education and training for the community and parents

Parents and the community should also be made aware of e-safety and the risks of social media, particularly as parents can play a critical role in minimising risks to children.

Depending on context, training and education may need to focus first on awareness raising. When auditing a project, it is helpful to be clear about the level of knowledge that parents and the community have about risks to children and young people online, and the safeguards that can be offered.

5. Standards – monitoring and reviewing the approach

An organisation's approach to e-safety needs to meet certain standards and be constantly monitored in order to minimise risks. Provision should be looked at against existing standards and constantly reviewed.

It is a good idea to carry out an annual audit, which will inform the review.

All e-safety incidents should be monitored and logged so that the organisation can review progress, and identify new risks.

There may also be a requirement to report and update e-safety issues to management boards and child safeguarding committees. However, whatever the external process, an organisation's approach to e-safety needs to be kept up to date to reflect advances in technology and skills.

Conclusions / Next steps

Overall access to social media is a valuable tool for all areas of the community but mitigating risk is crucial both in terms of life skills for children and young people but also in maintaining an organisation's role in protecting children and young people.

Appendices

1: E-safety checklist

Does your organisation:

- understand the e-safety issues and risks for the community they work with and have an audit?
- have policies in place that will protect children and young people and staff?
- have a broad strategy and approach to implementation that will lessen risks using the PIES model?
- understand the risks?
- have a nominated lead or e-safety contact person?

Do your staff and volunteers:

- receive ongoing training and support?
- know the reporting procedure for e-safety incidents (internally and externally)?
- understand the protocols on online behavior and interaction?
- consult with young people and the community about the development of policies and practices?
- understand how online safety relates to child protection and safeguarding and other policies and practices within the organisation?

Do your children and young people:

- understand online risks?
- have opportunities to practice appropriate online behaviour in a safe environment?
- know what your policy is about interacting online?
- engage in the development of policies and practices about their online safety?
- know how to protect themselves?
- understand how to report any issues that they have and who to contact?

Do parents and the community:

- understand how to support their children to help keep them safe online?
- understand how to manage risks and report online?
- know where to go and how to access help and support?

2: Legal context examples

Key international legislation which has relevance to online abuse includes:

- **UN Convention on the Rights of the Child (1989).** This sets out the civil, political, economic, social, health and cultural rights of children and is the most comprehensive statement of children's rights ever produced. By stating children's rights to protection from sexual abuse and freedom of expression, it can be linked to children's right to online protection.
- **Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (OPSC, 2000).** This makes direct reference to child pornography on the internet. It prohibits sale of children, child pornography and child prostitution, and obliges nations to pass laws within their own territories against these practices "punishable by appropriate penalties that take into account their grave nature".
- **Protocol to Prevent, Suppress and Punish Trafficking against Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organised Crime ('Palermo Protocol', 2000).** This commits states to prevent and combat trafficking in persons, protecting and assisting victims of trafficking and promotes cooperation among states in order to meet those objectives.
- **Council of Europe convention on cybercrime (2001).** This is the first international treaty seeking to address Computer and Internet crimes (dealing particularly with infringements of copyright, computer-related fraud, child abuse images, hate crime and violations of network security) by coordinating national laws, improving investigative techniques and increasing cooperation among nations.
- **Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007).** This is a multilateral Council of Europe treaty whereby states agree to criminalise forms of sexual abuse against children. It is the first international treaty that addresses child sexual abuse within the family. The Convention sets out a range of measures to prevent sexual exploitation and abuse, including the training and educating of children, monitoring offenders, and the screening and training of people who are employed or volunteer to work with children.

3: Template social media policy

See below a suggested outline for a social media policy. It should take into account the context of the organisation.

1. **Policy statement:** this describes what the policy covers, outlines standards for use of social media and cross-refers to other relevant policies, such as acceptable use of technology.
2. **Who the policy covers:** this section defines those covered by the policy, whether staff, volunteers, parents and children.
3. **The scope of the policy:** this states the need for staff to comply with the policy and outlines the consequences if they fail to do so. It cross-refers to policies relating to disciplinary procedure.
4. **Who is responsible for implementing the policy:** this section describes which people are responsible for overseeing, monitoring and updating the policy; contacts for questions about the policy; and emphasises that all staff and stakeholders should take responsibility for complying with the policy.
5. **Using social media sites:** this section states which people in the organisation are authorised to post and share material on social media sites using the organisation's name.
6. **Organisational requirements:** this section highlights guidance around specific areas, such as online communication between donors and sponsor children; use of images of children; use of personal information; promotion of the organisation; and rules regarding the use of social media.
7. **Use of work related social media:** this defines the social media that members of the organisation are allowed to use, such as Twitter. It also clarifies what staff and volunteers have to do before using social media, such as reading the policy, undergoing training, approval from managers and so on.
8. **Personal use of social media:** this section states whether the organisation allows personal use of social media where there are references to the organisation. If this is allowed, this section must spell out conditions of use, such as adherence to child safeguarding policies; disciplinary procedures; and disclaimers.

9. **Rules for the personal use of social media for staff and volunteers:**
   - Always write in the first person and use the disclaimer.
   - Never upload or post any defamatory, obscene, abusive or harmful content.
   - Inform the relevant member of staff if you observe another staff member uploading this type of content.
   - Do not share any sensitive information – name or location of a child or commercially sensitive information.
   - Always comply with the site/services terms of use.
   - You are personally responsible for the content that you share so always think about what you are posting and sharing.
   - Avoid posting personal information that identifies you.
   - Social media sites will be monitored and if staff are found in breach of the rules they are subject to disciplinary procedures as outlined in the disciplinary policy.
   - Misuse could have serious implications and could break the law especially in the case of child abuse images, defamation, harassment and bullying.
10. **Children and young people using the organisation's services:** this section spells out rules for the use of social media by children and young people, especially where they are being given access through an ICT project or encouraged to use social media.

    A significant number of social media sites require children to be over the age of 13 so the organisation should follow this requirement. Allowing children younger than 13 to use these sites would be a breach of terms and conditions.

    This section may emphasise particular points, for instance the need to ensure that young people are not identifiable, that they do not share their location; do not arrange to meet anyone they have encountered via social media, and that they always report suspicious contacts.
11. **Monitoring and reviewing the policy:** this final section should state how the policy will be reviewed , how often this will take place, and who is responsible for leading the review.

4: Sample end user acceptable use policy

_____ (Insert name of organisation/project) understands the importance of new technology for children and young people's development. However we recognise that relevant safeguards need to be put in place by the xx project to ensure children and young people remain safe whilst online or using social media.

We ask that all parents/carers/volunteers/responsible adult spend a few minutes to read through and discuss this policy with their child/children and then sign and return this form to the _____ (relevant contact at the local office) at the _____ (Insert name of project).

I will be responsible for my behaviour when using the internet and other online media at the organisation/project, including the resources I access and my use of language.

I will not deliberately browse, download or access material that could be considered offensive or illegal. If I accidentally come across any such material, I will report this to an adult.

I will not use social networking or the internet to send anyone material that could be considered threatening, offensive, upsetting, bullying or illegal.

I understand that my use of the internet and other online media on the projects ICT equipment can be monitored, logged and made available to my adults/volunteers and other staff members at the organisation/project. I will not give out any of my personal information such as name, age, address or telephone number.

I will not share my passwords with anyone else.

I will not arrange to meet someone unless accompanied by a member of staff or parent/carer.

I understand that these rules are designed to keep me safe and if they are not followed my parents/carers may be contacted.

We have discussed this policy and _____(Insert child's name) agrees to support the safe use of social at _____ (Insert name organisation/project). Parent's/carer's/volunteers name: _____ _____ (Insert name)

Parents/carer's/volunteers signature: _____ (Insert signature)

Date: _____ (Insert date)

Child's name: _____ (Insert child's name)

Child's signature: _____ (Insert child's signature)

Date: _____ (Insert date)

5: Code of conduct

A code of conduct for staff, volunteers and other professionals should include the following information:

1. Introduction

This section defines social media as well as introducing the code of conduct for staff and expectations around the code of conduct. It should:

- include a definition of social media: what it is and what it will be used for
- highlight that the code of conduct defines expectations and rules for the use of social media by staff, in work and outside
- relate to other policies concerned with safeguarding children generally.

2. Using social media outside work

This section defines staff protocol around the use of social media in personal time, emphasising that all use should be considered in relation to their professional work and that they are in a position of trust, working with potentially vulnerable children.

Therefore the following principles should be considered:

- Always demonstrate a positive postion.
- Be consistent – if staff and volunteers associate themselves with a project and/or organisation they should ensure that online postings are consistent with protocol.
- Always think twice about what you post and share and how it will reflect on you and the organisation.
- Use discretion in all personal communication and never claim that you are speaking on behalf of the organisation. Make it clear that it is a personal point of view. Use a disclaimer.
- Know your obligations, sanctions and rules when using social media.
- Consider child safeguarding policies and procedures and do not discuss individual cases.
- Always show respect and courtesy. Be respectful of fellow colleagues/volunteers and do not make derogatory comments.

3. Using social media for communication at work

This section should focus on how staff and volunteers should use social media for communication at work. It should make links to any strategy or policy the organisation has in place for the use of social media. This section might include statements such as:

- We encourage conversation between donors and the organisation.
- Dialogue through the use of social media is critical to the aims of the organisation, its development and growth. It is crucial in our effort to engage with people and to support our values. (Insert the values of the organisation here).
- We expect you to exercise personal responsibility whenever you participate in social media.
- This includes not breaching anybody's trust. Be sure that you are presenting accurate information and ensure nobody is misled.
- Each tool and medium has appropriate and inappropriate uses. We encourage all employees to join in conversations but it is important to understand what is recommended, expected and required when you discuss work related topics.
- Do not use any social media tool without proper consideration and, in some instances, provide a business case.

4. Guidance to employees

This section offers specific advice to professionals and volunteers about how they should use social media and what the expectations are.

It should consider the following:

- Training and whether or not it staff undertake training before using social media
- Agreement to abide by the code of conduct
- Transparency and honesty – the use of real names and pseudonymns.
- Declaration of vested interests.
- Following data protection and copyright laws.
- Asking permission before publicising information about the organisation.
- Always considering the values of the organisation.
- Being careful not to share personal information that makes you individually identifiable.
- Raising any issues and concerns and follow protocol relating to inappropriate comments or material.

6: Best practice communication between sponsors and sponsored children using social media

Managing communication between sponsors and sponsored children

Managing communication between sponsor children and donors is a challenge for many NGOs. The advent of social media and increasing uses of the internet, are bringing fresh challenges.

Keeping Children Safe, with the support of CEOP, World Vision and Plan, have developed a position on e-safety for NGOs, which highlights current best practice. Keeping Children Safe will review this position as social media, access and approaches evolve.

Currently Keeping Children Safe advise the following:

Principles:

1. The use of social media as a communication tool between donors and sponsor children should not be encouraged or permitted.
2. Where contact does happen there should be clear reporting routes for sponsor children, young people and for donors. For example, there should be a local point of contact for sponsor children within existing child safeguarding arrangements and through local area offices and this should be included in child safeguarding procedures and policies. For donors who are contacted via generic social media such as Facebook and Twitter, there should be a point of contact, which should given to them when they sign up and should be part of the guidelines.
3. Online contact should be treated the same way as physical contact, especially where the NGO is responsible for the relationship between the child and the donor. Safeguarding children is always at the heart of the arrangement. If an NGO is not mediating, contact should be absolutely forbidden and the reasons why made explicit to sponsor children, their families, the community, staff, volunteers and donors.

What does this mean in practice?

1. All NGOs should make explicit reference to social media contact in their sign up guidelines and the subsequent child safeguarding information they provide to donors. NGOs should state why this type of contact is risky and should educate donors on this basis. They should also consider how much personal information they share with sponsor children, their families and donors.

   At present, donors receive names and geographical location, though not always specific. Sponsor families receive full name and city location. NGOs should think about how much information they share because people can be found easily and identified even with sparse information.
2. All offline communications should be screened to make sure that digital information is not shared, for example: Skype names, emails, Facebook details and Twitter handles.
3. NGOs should consider and review their processes if donors are consistently trying to share information that makes them identifiable through social media. If donors consistently share information, their sponsorship should be reviewed and terminated.

4. Where there is a one-to-one donor and child sponsor relationship and therefore an imbalance of power, NGOs should go above and beyond the normal sponsorship sign up process, particularly given the rise in social media use. For example NGOs should consider insisting that donors make a declaration/agreement about their intentions and reveal any criminal convictions.
5. Staff, volunteers, children, donors and the community should be educated about the risks of contact via social media. This should be part of existing training arrangements for all parties and for donors and should be part of the induction arrangements.

Keeping Children Safe advocates "healthy online communication" but currently advises organisations not to set up networks whereby sponsor children and donors can communicate online.

Based on existing best practice for communication between children and adults, any NGO wanting to develop an online communication forum should implement the following:

Step 1 – Review current systems and processes to ensure they cover online safeguarding. Ensure that policies and practices include e-safety as a matter of course and that they are built into the mainstay of current activities and policies

Step 2 – Ensure that there is somebody who is responsible. Put somebody in charge of the project, ensure he or she is thoroughly trained and vetted and has an awareness and knowledge of child safeguarding and social media issues.

Step 3 – Find a safe and secure system. Develop a new system or use an existing one. Either way the system must be safe and secure. It should be a "closed" environment, and not public, and it should be fully moderated. Private messaging In this forum should be avoided because private messages cannot be checked and verified.

Technical solutions such as filtering should be used so that no personal information can be shared.

Step 4 – Moderation. NGOs should only use online networks that are moderated by fully trained and qualified staff. Staff must be vetted and checked. Avoid networks that do not use human moderators.

If using an existing system ensure that all comments and sharing can be moderated prior to publishing and making visible.

Step 5 – Escalation and flagging. Escalation and flagging systems should be in place including relationships with 3rd parties – police, other NGOs and local services.

Step 6 – Privacy. NGOs should ensure that the highest levels of privacy are set for children and young people and for staff on forums so that no personal information is shared or publicly available.

Step 7 – Education. Children, young people, staff, parents and the community should be educated about the risks before they sign up to the use of the service. Education should be ongoing so users develop confidence and resilience.

7. The principles of healthy online communication

Children and young people need to learn the principles, behaviours and practices for healthy online communication so they can minimise risks and protect their digital footprint.

Organisations that are promoting the use of social media have a duty to teach young people how to use the internet and social media responsibly and safely.

In order to facilitate healthy online communication, all organisations should educate young people in key areas.

- Rights and responsibilities: plan suitable activities for children, which enable them to understand their rights online and, similarly, encourage responsible behavior.
- Encourage young people to "think before they post". Encourage them to participate in offline case studies, then apply what they have learned to the online world.
- Offer guidance in creating a responsible online profile.
- Ensure young people understand what personal information is and how they can protect it. Provide guidance on what is and is not appropriate sharing of personal information.
- Ensure they know where to find help and support and encourage young people both to support each other and to report inappropriate content.
- Respect the law and encourage them to know their own limitations.
- Encourage children and young people to use online communication positively for promoting and sharing ideas and healthy social interaction.
- Emphasise that most online interaction is positive and their influence online can be very valuable.

For more information, resources and advice visit the following web sites

- www.childnet.com
- www.ceop.gov.uk
- www.fosi.org
- www.unicef.org/ceecis/resources_18475.html
- www.wvi.org/keeping-children-safe-online
- www.saferinternet.org
- www.saferinternetcentre.org.uk

All children, whoever they are and wherever they are, have a right to be protected.

www.keepingchildrensafe.org.uk

info@keepingchildrensafe.org.uk

Charity registration number: 1142328 / © Keeping Children Safe 2014

Photography: Keeping Children Safe/Sven Torfinn, Keeping Children Safe/ Ben Troester, Keeping Children Safe/Sven Torfinn, Keeping Children Safe/Ben Troester

Design: www.wave.coop