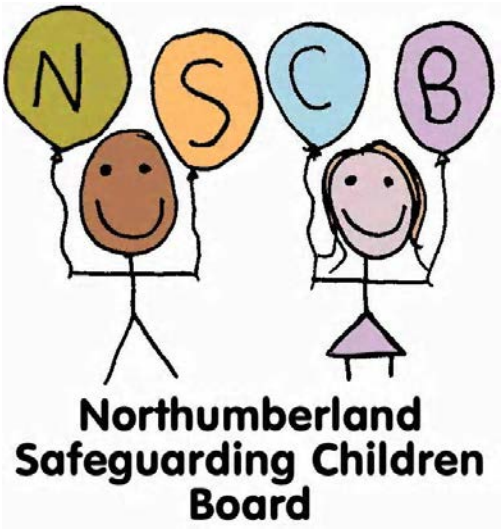

E-SAFETY – SOCIAL MEDIA GUIDANCE

for people who work with Children and Young People

Document control and record of amendments

Version	Reason for amendment	Amended by/ Date
1	New guidance – ratified by NSCB in October 2014	May 2014

Contents

What do we mean by Social Media?

The term Social Media is used in a number of ways, but for the purposes of this guidance, is defined as any electronic communication that enables people to stay in touch online. Social Media includes web and mobile based technology which are used to turn communication into interactive dialogue between organisations, communities and individuals. Social media provides support for sharing information, images and making contact with people who may share a common interest.

Introduction

The purpose of this guidance is to provide a building block for organisations to develop their own advice and guidance about safer working practice in relation to social media, keeping personal and professional lives separate, keeping safe when using electronic media and adopting responsible behaviour that should protect staff from putting themselves and their career at risk.

This document is guidance only, it is not intended to interfere in an employees private life, but to help avoid work and private lives clashing in inappropriate ways because of social networking activities. It should be read in conjunction with the relevant policy within your own employing organisation.

Northumberland Safeguarding Children Board (NSCB) expect all member agencies to have policies in place to support e-safety practice. The following list is not exhaustive:

- Data Protection Policy
- Information Governance Policy
- Code of Conduct
- ICT Security Policy
- **Social Media Policy** for staff, which is congruent with this guidance and includes the requirement to maintain appropriate professional standards both inside and outside of the work environment (e.g. Social Networking Sites)
- Appropriate **Acceptable Use Policies (AUP)** which users must read (and sign where applicable) before using any ICT resources.

Background

Digital technology has become an important part of everyday life and offers exciting opportunities. However the increasing number of cases where workplace practice has highlighted inappropriate use of technology, grooming behaviour and an inability to challenge colleagues has demonstrated the need for clear practice guidance for workers and organisations around safer working practice in this area.

This guidance builds on the ‘Safer Working Practice Guidance for adults working with children and their Families’ issued by the Government Offices in England in 2007.

As someone who works with children and young people, or adults who are their parents and carers, whether in a voluntary or paid capacity, whenever you are operating in the digital world you must always have your professional role in mind and always consider how your behaviour could affect your professional reputation and employment. **All digital records should be considered to be permanent.**

Legal Consequences

All staff and volunteers who have access to online services through work networks should be reminded of the legal consequences attached to the inappropriate use of those services. Although this list in not exhaustive examples of inappropriate or offensive material include racist material, pornography, sexually explicit images, texts and related material, the promotion of illegal activity, or intolerance of others.

Offences Committed on Social Networking Sites, Email, Mobile Technology & the Internet

Threats to kill

Conviction of a Summary Offence: A fine and/or a maximum of 6 months imprisonment

Conviction of an Indictable Offence: 10 years in prison

Intended harassment of another person

Conviction of a Summary Offence: A fine and/or a maximum 6 months in prison

Putting a person in fear of violence

Conviction of a Summary Offence: A fine and/or maximum of 6 months in prison

Conviction of an Indictable Offence: A fine and/or a maximum of 5 years imprisonment

Intending to cause distress or anxiety by sending indecent, offensive or threatening letters, electronic communication or other articles to another person

Conviction of a Summary Offence: A fine and/or maximum of 6 months in prison

Threats to destroy or damage property

Conviction of a Summary Offence: A fine and/or a maximum of 6 months imprisonment

Conviction of an Indictable Offence: 10 years in prison

Causing intentional harassment, alarm or distress

Conviction of a Summary Offence: A fine and/or maximum of 6 months in prison

Summary offences include less serious offences. (Magistrates' Court).
Indictable offences are more serious. (higher court by a judge and jury).

Recent Case Law

Recent case law which has raised the media spotlight to the subject matter include:

"A manager was verbally abused by two customers where she worked. She dealt with the situation in a professional manner at the time but later, while still at work, vented her frustrations via Facebook making a number of abusive and inappropriate comments. The comments were seen by the customers' daughter who saw them and complained.

The manager was dismissed for gross misconduct as it was judged that she had brought her employer into disrepute by posting derogatory comments. The manager believed that her privacy settings would have prevented anyone other than family and friends from seeing the comments."

"An employee was opposed to the changes in terms and conditions that would have required him to work 3 weekends out of every 4. He was off sick during the consultation period but decided to start a Facebook page campaigning against the changes to terms and conditions.

The employee was disciplined for making public statements that encouraged dissent in the workplace and were not in the company's interests."

"A Community Psychiatric Nurse was struck off in September 2010 for conducting an inappropriate relationship with a former patient. He had met her when she attended a screening assessment, and offered her counselling and support. He contacted her through Facebook two weeks after she was discharged; they saw each other regularly and developed a sexual relationship."

Please use the following pages as guidelines. They have been developed as a communication tool for your organisation. It is envisioned that the following pages can be used on notice boards and/or as posters. Please adapt for your organisations requirements.

General guidelines –

- Remember you are responsible for the data on your electronic communication device
- DO NOT behave in a way that could suggest that you are trying to develop a personal relationship with a child or vulnerable adult
- DO NOT post any content that could be deemed defamatory, obscene or libellous
- DO NOT post comments that exhibit or appear to endorse grossly irresponsible behaviour or law breaking of any kind

☑ Appropriate

1. Set your privacy settings for any social networking site.
2. Ensure any technological equipment, (including your mobile phone) is password/ PIN protected.
3. Consider having professional online accounts/ identities if you wish to have online contact with service users, their families and other professionals.
4. Make sure that all publicly available information about you is accurate and appropriate
5. Remember online conversations may be referred to as 'chat' but they are written documents and should always be treated as such.
6. Make sure that you know the consequences of misuse of digital equipment.
7. If you are unsure who can view online material, assume it is public. Remember - once information is online you have relinquished control.
8. Switch off Bluetooth
9. When you receive any new equipment (personal or private) make sure that you know what features it has as standard and take appropriate action to disable/ protect.

☒ Inappropriate

1. Give your personal information to service users -children/ young people, their parents/ carers. This includes mobile phone numbers, social networking accounts, personal website/ blog URLs, online image storage sites, passwords etc.
2. Use your personal mobile phone to communicate with service users. This includes phone calls, texts, emails, social networking sites, etc.
3. Use the internet or web-based communication to send personal messages to children/young people
4. Share your personal details with service users on a social network site
5. Add/allow a service user to join your contacts/friends list on personal social networking profiles.
6. Use your own digital camera/ video for work. This includes integral cameras on mobile phones.
7. Play online games with service users.

We recommend the above as good practice, these will be subject to management approval and local organsiational policies.

For fuller statements go to P13 & 14

Social Networking

Facebook and Twitter are the most well known packages but other packages include BEBO (Blog Early, Blog Often), MySpace, Yahoo, LinkedIn and MSN. These are not exhaustive. Remember: **Host privacy settings often change – keep track of yours**.

Don't use your personal social network profile to communicate with or share images or take images of children/ young people and their parents/ carers

Either using your personal or organisational equipment

Don't accept children and young people/ parents and carers as friends on your personal page.

Best practice

Consider creating a professional profile in agreement with your manager/ organisation.

Young people may have several profiles themselves (personal and one for parents to see) so will appreciate this approach.

Make sure that you don't have links to your personal profile (this defeats the object!)

Make sure your security settings are not open access.

Safe practice

Make sure your security settings are not open access - set to family and friends only

Don't accept people you don't know as friends – they could be service users. Go for quality not quantity.

Be aware that belonging to a 'group' can be a 'back door' into your profile.

Ask your family and friends to protect your professional status and not post tagged images of you on their open access profiles

May affect your relationship with service users. May affect professional status through professional body concerns about bringing the profession into disrepute

Poor practice

You have an open access profile that includes inappropriate personal information and images e.g. holiday snaps, hen nights

You accept service users as friends on your personal profile once work is completed. Other service users may gain access to your profile.

You collect 'friends' including people you don't know in real life.

You use your personal profile to communicate with service users without your manager's knowledge or permission.

Breach of AUP. May make you vulnerable to harassment, bullying or allegations. Disciplinary/ capability processes may be instigated.

What should be in place?

- The AUP should explicitly state that children/ young people and their parents/ carers should not be accepted as friends and include sanctions for the breach of this policy.
- The AUP for the organisation should include guidelines for creating/ monitoring a separate professional profile if this is considered an appropriate way of working.
- The AUP is part of the induction process and includes advice about the need for a professional online presence

Email

Don't use your personal email account to communicate with children/ young people, their parents/ carers and adults who may be at risk

Either via mobile phones or web based software

Best practice

Your organisation should provide an email account for you to use for professional communications.

Safe practice

Check your organisation policy regarding use of your work account for personal use e.g. shopping.

Poor practice blurs the professional boundaries and can make workers vulnerable to bullying/ harassment/ allegations. If it's a breach of the AUP then it may result in capability/ disciplinary proceedings

Poor practice

You use your personal email account to communicate with service users and their families without manager's knowledge or permission.

You retain emails for your personal use.

What should be in place?

- AUP should be explicit about use of personal email accounts to communicate with service users.
- AUP should be explicit about using work accounts for personal purposes.
- AUP should include sanctions for breaching the policy.

Images (still and moving)

Don't use your own equipment to take images of children/ young people

This includes built in equipment on mobile phones, standalone cameras/ video recorders.

Best practice

Your organisation should provide equipment for you.

Know who/ where to get equipment from.

Safe practice

Senior managers agree you can use your own equipment.

You make arrangements for pictures to be downloaded to organisation network immediately after the event.

May result in capability/ disciplinary proceedings

Poor practice

You download images from organisation equipment to your own equipment.

You use your own equipment without manager's knowledge or permission.

You retain images for your personal use and don't delete them from your equipment.

What should be in place?

- Use of personal equipment should be made clear in AUP
- Taking images/moving images of service users and the distribution and hosting of these should be included in AUP. Consent has been obtained which includes taking images and use of images e.g. on website, displays etc
- Workers know where equipment is available from and should be returned, who is responsible for downloading onto organisation's storage and deleting from camera.

Mobile Phones

Don't use your personal mobile phone to communicate with children/ young people, their parents/ carers and adults who may be at risk.

This includes phone calls, text messages, email or web-based communications e.g. Twitter

See page 11 & 12 for further guidance

Best practice

Your organisation should provide equipment for you.

Know who/ where to get equipment from.

Make sure you know about inbuilt software/ facilities and switch off if appropriate

Safe practice

Senior managers agree you can use your own equipment.

Make sure you know about inbuilt software/ facilities and switch off if appropriate

Consider changing your number.

Service users having your personal details may make you vulnerable to harassment or

Poor practice

You use your own equipment without manager's knowledge or permission.

You retain service user contact details for your personal use.

Misuse of personal information may be a breach of the AUP. Workers may be vulnerable to allegations as well as capability/ disciplinary process

What should be in place?

- Use of personal equipment should be made clear in AUP
- If the need for a mobile phone is for a one-off situation e.g. trip then workers know where equipment is available from and should be returned, make sure that it is fully charged and has sufficient credit.
- If the phone is to be used abroad then check that the phone has roaming access.

Live Streaming Media

For example Web cams or video conferencing. Facetime and Skype are the most well known packages but there are many more packages in development, Therefore these are not exhaustive.

Don't use your personal web-cam to communicate with children/ young people, their parents/ carers or to make a record of activity without permission

Best practice

Make sure you know about inbuilt software/ facilities and switch off.

Safe practice

Senior managers agree you can use your own equipment for a specific project.

You make arrangements to download to the organisation network immediately after the event.

Misuse of personal information may be a breach of the AUP. Workers may be vulnerable to allegations as well as capability/ disciplinary process

Poor practice

You use your own equipment without manager's knowledge or permission.

You retain service user information/ activity for your personal use.

What should be in place?

- Use of personal equipment including webcams should be made clear in AUP
- If the need to use a webcam is for a one-off situation e.g. project, then appropriate organisational safeguards need to be in place.
- Arrangements must be made for storing the work on the organisation's network immediately following the activity

Using the Internet

Be aware of the organisation policy for the use of the internet on your work computer.

Security software may mean that some sites are blocked or restricted access.

Best practice

Appropriate software to ensure safe and secure access to the web is installed

Understand how to search safely online and how to report inappropriate content either via your organisation's ICT section or via the CEOP report button

Safe practice

Be aware that the organisation's monitoring software will log your activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians

Misuse of personal information may be a breach of the AUP. Workers may be vulnerable to allegations as well as capability/ disciplinary process

Poor practice

Accessing or downloading inappropriate or illegal material may result in criminal proceedings.

Breach of the AUP may result in confiscation of equipment, closing of accounts and instigation of capability/ disciplinary processes.

What should be in place?

- AUP make explicit the consequences/ sanctions for inappropriate use of the internet.

Summary of Good Practice Guidelines

☑ APPRORIATE

1. Set your privacy settings for any social networking site to ensure only the people you want have sight/ access to the contents. Keep these updated. The default settings for most social networking sites are set to open access where anyone can see everything.

2. Ensure your mobile phone (any technological equipment) is password/ PIN protected. This will ensure that other people can't use your equipment and get you into trouble.

3. Consider having separate personal and professional online identities/ accounts if you wish to have online contact with service users i.e. children and young people, their families and other professionals. Ensure that your manager is aware of your professional online persona.

4. Make sure that all information about you that is publicly available is accurate and appropriate – think particularly about whether photographs/ stories that you may have posted in your personal life are appropriate for a person with a professional life and a reputation to lose. If you don't want it to be public, don't put it online.

5. Remember that online conversations may be referred to as 'chat' but they are written documents and should always be treated as such. Be mindful about how you present yourself when you are publishing information about yourself or having 'conversations' on-line.

6. Make sure that you are aware of your organisation's policy regarding the use of both organisational and personal digital equipment and the consequences of misuse. Breach of the policy can result in capability/ disciplinary actions by your employer, professional body and criminal proceedings by the police.

7. Err on the side of caution. If you are unsure who can view online material, assume that it is publicly available. Remember - once information is online you have relinquished control of it. Other people may choose to copy it, to edit it, to pass it on and to save it.

8. Switch off any Bluetooth capability any device may have installed as standard. Bluetooth allows another person to have access to your equipment – they can then pretend to be you.

9. Always be aware that technology is constantly upgrading and improving. You may have access to websites via a work-provided smart phone that are blocked by your computer. Mobile phones come with locator software. Cameras can be a feature of games consoles. When you receive any new equipment (personal or private) make sure that you know what features it has as standard and take appropriate action to disable/ protect.

☒ INAPPROPRIATE

1. Give your personal information to service users i.e. children/ young people, their parents/ carers. This includes personal mobile phone numbers, social networking accounts, personal website/ blog URLs, online image storage sites, passwords/ PIN numbers etc.

2. Use your personal mobile phone to communicate with service users i.e. children/young people or parents/carers either by phone call, text, email, social networking site.

3. Use the internet or web-based communication to send personal messages to service users i.e. children/young people, parents/ carers.

4. Share your personal details on a social network site with service users i.e. children/young people, their parents or carers. This includes accepting them as friends. Be aware that belonging to a 'group' may give 'back door' access to your page even though you have set your privacy settings to family and friends only.

5. Add/allow service users i.e. a child/young person, their parents/ carers to join your contacts/friends list on personal social networking profiles.

6. Use your own digital camera/ video for work. This includes integral cameras on mobile phones.

7. Play online games with service users i.e. children, young people, their parents or carers. This can be difficult when the culture is to play with '*randoms*'. Check out before you play online with someone you don't know.

Template for Development of Organisational Social Media Policy

The enclosed template is provided as a starting point for organisations wanting to develop their own policy. It is not prescriptive. Please adapt as suits your organisation.

DRAFT - Model Social Media Policy.doc

What to do if you have concerns

As a user of social networking site, you may at some time have a concern about what you are seeing or being told about by another user. Concerns may range from negative or abusive comments and cyber bullying to suspected grooming for sexual abuse.

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

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 following reports:

'Safer Children in a Digital World'.

Safer Children in a Digital World: A summary for children and young people

Do we have safer children in a digital world? A review of progress since the 2008 Byron Review

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-int.org

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 ChildLine 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 websites' 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.
http://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/publications/operational-policing/social-networking-guidance/

Guidance for the Moderation of Interactive Services for Children

http://police.homeoffice.gov.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

Child Protection in Sport Unit (CPSU)

The CPSU provides a range of services to support partners in the sports sector including:

- safeguarding briefings and updates
- development and delivery of training and learning resources
- supporting organisations to put effective systems and structures in place.

www.thecpsu.org.uk

CPSU Briefing on Photographs and Images of Children

The NSPCC's Child Protection in Sport Unit (CPSU) has created a briefing that gives guidelines on using photographs of children and has a sample permission form for children and parents.
http://www.nspcc.org.uk/Inform/cpsu/Resources/Briefings/PhotographsAndImagesOfChildren_wdf60645.pdf

Cyberbullying

The Teachernet site has a wealth of information on cyberbullying.
www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/

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.org.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.teachtoday.eu