Social Networking Policy

This is an approved North Somerset Safeguarding Children Board document and should not be edited in any way.

Reference Number: NSSCB/LP/008
Target Audience: Multi-agency
Sources of advice in relation to this document:
Replaces if appropriate:
Type of Document: Policy
Approved by: Independent Chair NSSCB and Board Manager
Date: 23 January 2017
Date displayed on NSSCB web site: 23 January 2017
Date due to be reviewed by responsible person or body: January 2018

Section 1: Introduction

1.1 Objectives

1.1.1 This policy sets out North Somerset's Safeguarding Children Board's policy on social networking. This document aims to:

- Assist adults working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Support safer working practice
- Minimise the risk of misplaced or malicious allegations made against adults who work with children and young people
- Prevent adults abusing or misusing their position of trust

1.1.2 Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances adults will always advise their managers of the justification for any such action already taken or proposed. Managers will in turn seek advice from their HR team where appropriate.

1.1.3 This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of employers and current relevant legislation.

1.2 Scope

1.2.1 This document applies to all adults who work or volunteer in NSSCB agencies and organisations. This includes paid staff, contractors and volunteers.

1.2.2 It should be followed by any adult whose work brings them into contact with children and young people during the course of their work/volunteer activities.

1.2.3 This policy should not be used to address issues where other policies and procedures exist to deal with them. For example any alleged misconduct which falls within the scope of the allegations management policy requires the agency to comply with additional child protection requirements as set out in that policy.

1.3 Status

1.3.1 This document does not replace or take priority over advice given by agency HR or code of conduct, dealing with allegations of abuse, other policies issued around safeguarding or IT issues (email, ICT and data protection policies), but is intended to both supplement and complement any such documents.

Principles

- Adults who work with children and young people are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions.
- Adults should work and be seen to work, in an open and transparent way.
- Adults should continually monitor and review their practice in terms of the continually evolving world of social networking and ensure they follow the guidance contained in this document.

Section 2: Safer Social Media Practice

2.1 What is social media?

2.1.1 For the purpose of this policy, social media is the term commonly used for websites which allow people to interact with each other in some way – by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook are perhaps the most well known examples of social media but the term also covers other web based services such as blogs, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as YouTube and micro blogging services such as Twitter. This definition of social media is not exhaustive as technology develops with new ways of communicating advancing every day.

2.1.2 For the purpose of this document the terminology Social Media is not exhaustive and also applies to the use of communication technologies such as mobile phones, cameras, PDAs / PSPs, tablets or other handheld devices and any other emerging forms of communications technologies.

2.2 Overview and expectations

2.2.1 All adults working with children and young people have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children and young people. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, children and young people, public in general and all those with whom they work in line with the agency's code of conduct. Adults in contact with children and young people should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.

2.2.2 This guidance sets out expected behaviours of adults who work with or have contact with children and young people. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them.

2.2.3 Organisations should also have clear policies in place relating to child protection; allegations management; use of both personal and agency equipment i.e. emails addresses; camera's etc. This will help ensure that individual's are aware of expectations regarding interaction and contact with children.

2.2.3 Adults within their work setting should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.

2.3 Safer online behaviour

2.3.1 Managing personal information effectively makes it far less likely that information will be misused.

2.3.2 In their own interests, adults need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for children, young people or their families or friends having access to the adult outside of the work environment. It also reduces the potential for identity theft by third parties.

2.3.3 All adults, particularly those new to the agency, should review their social networking sites when they join to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the agency if they are published outside of the site.

2.3.4 Adults should never make a 'friend' of a child or young person where they are working on their social networking page, and should not become 'friends' with children or young person no longer receiving a service. Working to the organisations policy on this will assist in reducing the possibility that being 'friends' with young person no longer in receipt of services will be called into question.

2.3.5 Adults should never use or access social networking pages of children and young people and should never accept an invitation to become a 'friend' of a child or young person. Where this has been requested the adult should inform their manager who will decide whether to discuss with the child's parents/carers.

2.3.6 Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site about themselves, their employer, their colleagues, children and young people or members of the public.

2.3.7 Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, children, young people or other individuals connected with the agency/organisation could result in formal action being taken against them.

2.3.8 Adults are also reminded that they must comply with the requirements of equalities legislation in their on-line communications.

2.3.9 Adults must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the agency into disrepute or could reflect negatively on their professionalism. Where derogatory, racist, or other inappropriate comments are made, these should be referred to the Designated Officer for Allegations in the Local Authority (formally known as the Local Authority Designated Officer - LADO) for consideration as to whether a criminal offence has taken place and regarding the individuals suitability to work with children.

2.3.10 Some social networking sites and other web-based sites have fields in the user profile for job title etc. Adults should not put any information onto the site that could identify either their profession or the agency where they work. In some circumstances this could damage the reputation of the agency or their profession.

2.4 Protection of personal information

Adults should:

2.4.1 Ensure that they do not use agency ICT equipment for personal use, e.g. camera or computers.

2.4.2 Keep their personal phone numbers private and not use their own mobile phones to contact children, young people or parents.

2.4.3 Never share their work log-ins or passwords with other people.

2.4.4 Not give their personal e-mail addresses to children, young people or parents. Where there is a need for correspondence or written information to be sent electronically the work e-mail address should be used.

2.4.5 Keep a record of their phone's unique international mobile equipment identity (IMEI) number and keep their phone secure whilst on their own and other organisations premises.

2.4.6 Understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.

2.5 Communication between children, young people / adults

2.5.1 Communication between children, young people and adults by whatever method, should take place within clear and explicit professional boundaries.

2.5.2 This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.

2.5.3 The agency may provide a work mobile and e-mail address for communication between adults and children/young people where this is necessary for particular trips/assignments. Adults should not give their personal mobile numbers or personal e-mail addresses to children/young people or parents.

2.5.4 Adults should not request, or respond to, any personal information from a child/young person, other than that which might be appropriate as part of their professional role.

2.5.5 Adults should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with children/young people so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual, financial or emotional exploitation.

2.5.6 Adults should not give their personal contact details to children/young people including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. Where agreed, the purpose of contact should be explicit, and access to such correspondence should be available to managers for review.

2.5.7 E-mail or text communications between an adult and a child/young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. Internal e-mail systems should only be used in accordance with the agency's policy.

2.6 Social contact

2.6.1 Adults should not establish or seek to establish social contact via social media /other communication technologies with children or young people.

2.6.2 There will be occasions when there are social contacts between children/young people and adults, where for example the parent and adult are part of the same social circle. These contacts however, will be easily recognised and should be openly acknowledged with their manager where there may be implications for the adult and their position within the agency setting.

2.6.3 There must be awareness on the part of those working with or in contact with children/young people that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social networking contacts made through outside interests or through the adult's own family.

2.6.4 Where a parent who has accessed the organisations services becomes a volunteer or paid employee it will be important to ensure that they are clear on the organisations expectations regarding ongoing relationships and developing professional boundaries with children and their parents who continue to access the service. As such they should also be expected to work within and apply this protocol.

2.7 Access to inappropriate images and internet usage

2.7.1 There are no circumstances that will justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and disciplinary action being taken.

2.7.2 Adults should not use equipment belonging to their agency to access any adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with and associated risk to children.

2.7.3 Adults should ensure that children/young people are not exposed to any inappropriate images or web links. Agencies need to ensure that internet equipment used by children/young people have the appropriate controls with regards to access e.g. personal passwords should be kept confidential.

2.7.4 Where indecent images of children are found, the police and local authority Designated Officer for Allegations (formally known as the Local Authority Designated Officer - LADO) should be immediately informed. Agencies should refer to the Allegations Management policy on the NSSCB website and should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated or compromised which in itself can lead to a criminal prosecution.

The individual should not be confronted or otherwise informed of the discovery of indecent images as this may lead to destruction of evidence or increased risk to children or compromise a criminal investigation. The Designated Officer for Allegations and police will advise of the process and timing of any investigation.

2.7.5 Where other unsuitable material is found, which may not be illegal but which raises concerns about that adult, either HR or the Designated Officer for Allegations should be informed and advice sought. Agencies should refer to the Allegations investigate or evaluate the material themselves until such advice is received.

2.8 Cyberbullying

2.8.1 Cyberbullying can be defined as ‘the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.’

2.8.2 Prevention activities are key to ensuring that adults are protected from the potential threat of cyberbullying. All adults are reminded of the need to protect themselves from the potential threat of cyberbullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

2.8.3 If cyberbullying does take place, records should be kept of the abuse such as text, e-mails, website or instant messages and texts or e-mails should not be deleted. Adults are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.

2.8.4 Adults may wish to seek the support of their trade union or professional association representatives or another colleague to support them through the process.

2.8.5 Adults are encouraged to report all incidents of cyberbullying to their line manager. All such incidents should be taken seriously and dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

2.8.6 Equally Adults need to be very clear that any online activity they undertake that may be considered bullying of another person, whether child or adult, or any threatening statements will be considered a disciplinary matter and may lead to criminal investigation and conviction. This is regardless of whether the behaviour has occurred within or outside of work, on work or personal equipment.

Section 3: Link with other policies

3.1.1 This document should be read in conjunction with their organisations relevant policies on;

- IT and security standards
- Disciplinary Policy and Procedures
- Equal Opportunities Policy
- Code of Conduct

3.1.2 All adults must adhere to, and apply the principles of this document in all aspects of their work. Failure to do so may lead to action being taken under the disciplinary procedure.

Section 4: Review of policies

4.1.1 Due to the ever changing nature of information and communication technologies it is best practice that organisational policies be reviewed annually and, if necessary, more frequently in response to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

Appendix A – Relevant legislation

Adults should be aware of the legislative framework which currently surrounds use of social media / communication technology in the UK. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Computer misuse act 1990
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;

- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data protection act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Not transferred to other countries without adequate protection.

Freedom of information act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious communications act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.
Regulation of investigatory powers act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.

- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, designs and patents act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal justice & public order act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and religious hatred act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from harassment act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of children act 1978 12

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise).

Sexual offences act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) and you arrange to meet them or travel to meet them (anywhere in the world) with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in any sexual activity with any person under
18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public order act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene publications act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human rights act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The organisation is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.