

KILDWICK CE PRIMARY SCHOOL
Striving for Excellence and Promoting Christian Values
Social Networking Policy

Date Approved: March 2017	Next Review: March 2018
----------------------------------	--------------------------------

Section 1: Introduction

- 1.1 Objectives
- 1.2 Scope
- 1.3 Status
- 1.4 Principles

Section 2: Safer Social Media Practice in Schools

- 2.1 What is social media?
- 2.2 Overview and expectations
- 2.3 Safer online behaviour
- 2.4 Protection of personal information
- 2.5 Communication between pupils / schools staff
- 2.6 Social contact
- 2.7 Access to inappropriate images and internet usage
- 2.8 Cyber bullying

Section 3: Links with other school policies

Section 4: Review of policy

1.1 Objectives

1.1.1 This policy sets out Kildwick CE VC Primary School's policy on social networking.

New technologies are an integral part of our lives and are powerful tools which open up teaching and learning opportunities for schools' staff in many ways. This document sets out Kildwick CE VC Primary School's policy on social networking and aims to:

- Assist schools' staff 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 pupils.
- 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 staff in schools will always advise the Headteacher of the justification for any such action already taken or proposed. The Headteacher will in turn seek advice from the Schools' HR team where appropriate.

1.2 Scope

1.2.1 This document applies to all adults who work at Kildwick CE VC Primary School as adopted by the governing body. This includes teachers, support staff, supply staff, governors, contractors, kitchen staff and volunteers.

1.2.2 It should be followed by any adult whose work brings them into contact with pupils. References to adults should be taken to apply to all the above groups of people in schools. Reference to pupils means all pupils at the school including those over the age of 18 or those who are on work experience or University placement.

1.3 Status

1.3.1 This document does not replace or take priority over advice given by Children's Services HR, the School's Child Protection policy or other policies issued around safeguarding or IT

1.4 Principles

- Adults who work with pupils 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 in schools should work and be seen to work, in an open and transparent way.
- Adults in schools 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 in Schools

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. The social networking website, Facebook is 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, iPads or other handheld devices and any other emerging forms of communications technologies.

2.2 Overview and expectations

2.2.1 All adults working with pupils have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils or students, public in general and all those with whom they work in line with the school's Child Protection Policy. Adults in contact with pupils 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 The guidance contained in this policy is an attempt to identify what behaviours are expected of adults within the school setting who work with or have contact with pupils. Anyone whose practice deviates from this document and/or their professional or employment-related codes 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 Adults within the school 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 within school settings 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 pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

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

2.3.4 ***Adults should never make a 'friend' of a pupil at Kildwick CE VC Primary on their social networking page, or with ex-pupils under the age of 18.***

2.3.5 ***Staff should never use or access social networking pages of pupils and should never ask a pupil to become a 'friend'.***

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, pupils 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, pupils or other individuals connected with the school, or another school 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 within the school setting must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the school into disrepute or could reflect negatively on their professionalism.

2.4 Protection of personal information

Adults working in schools should:

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

2.4.2 Keep their personal phone numbers private

2.4.3 Not give their personal e-mail addresses to pupils or parents, the school e-mail address should be used. (admin@kildwick.n-yorks.sch.uk or staff email address <name of teacher>@kildwick.n-yorks.sch.uk)

2.4.4 Keep your phone secure whilst on school premises.

2.4.5 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.

2.4.6 Download and delete the same day any photographs taken on personal equipment.

Adults working in schools should not:

2.4.6 Use school ICT equipment for personal use, e.g. camera or computers.

2.5 Communication between pupils / adults working in school

2.5.1 Communication between pupils and adults by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.

2.5.2 Adults should not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.

2.5.3 Adults should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with pupils so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending.

2.5.4 Adults should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. For example, in extreme cases when on residential visits where an adult maybe working with a child on the SEN register.

2.5.5 E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

2.6 Social contact

2.6.1 Adults should not seek to establish social contact via social media / other communication technologies with pupils.

2.6.2 There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and should be openly acknowledged with the Head Teacher where there may be implications for the adult and their position within the school setting.

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. Staff 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 the disciplinary action being taken.

2.7.2 Adults should not use equipment belonging to their school/service 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 children.

2.7.3 Adults should ensure that pupils are not exposed to any inappropriate images or web links. Schools need to ensure that internet equipment used by pupils 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 (LADO) should be immediately informed.

Schools should refer to the dealing with allegations of abuse against adults' policy and should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

2.7.5 Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff, either HR or the LADO should be informed and advice sought. Schools should not attempt to investigate or evaluate the material themselves until such advice is received.

2.8 Cyber bullying

2.8.1 Cyber bullying 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 cyber bullying. All adults are reminded of the need to protect themselves from the potential threat of cyber bullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

2.8.3 If cyber bullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Employees 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 cyber bullying to the Headteacher. All such incidents will be taken seriously and will be 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.

Section 3: Link with other policies

3.1.1 This document should be read in conjunction with the following school/ documents:

- Disciplinary policy and procedures
- Equal opportunity policy
- Child Protection Policy
- ICT Acceptable use agreement

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 policy

4.1.1 Due to the ever changing nature of information and communication technologies it is best practice that this policy 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.