LSCB

Bath & North East Somerset
Local Safeguarding Children Board

Batheaston Primary School
Social Media Policy

Date approved by LSCB Update ratified by FGB	August 2016
Author Jackie Deas and Hester Edmond	Original Author: Review Author – Nikki Macbeth
Date for review	May 2018
Detail of review amendments	

Contents **2**

Section 1: Introduction

1.1 Objectives

1.1.1 This policy sets out Batheaston Primary School policy on the use of social media. Social Media is an integral part of our lives and a powerful tool which opens up teaching and learning opportunities for schools' staff in many ways. This document sets out Batheaston Primary School policy on the use of social media and aims to:

- **Assist schools' staff working with pupils 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 their headteachers of the justification for any such action already taken or proposed. Headteachers will in turn seek advice from the Schools' HR Provider where appropriate.

1.1.3 This policy takes account of employment legislation and best practice guidelines in relation to the use of social media in addition to the legal obligations of governing bodies and the relevant legislation listed at appendix A.

1.2 Scope

1.2.1 This document applies to all adults who work in Batheaston Primary School as adopted by the governing body. This includes teachers, support staff, supply staff, governors, contractors 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.

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 management of allegations policy requires the school to comply with additional child protection requirements as set out in that policy.

1.3 Status

1.3.1 This document needs to sit alongside the relevant school's safeguarding policies and codes of conduct. The Local Safeguarding Children's Board and the Local Authority supports the use of Guidance for safer working practice for those working with pupils in education settings.

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 media and ensure they follow the guidance contained in this document.

Section 2: Safer Social Media Practice in Schools

2.1 Communication with children (including the use of technology)

2.1.1 In order to make the best use of the many educational and social benefits of new and emerging technologies, pupils need opportunities to use and explore the digital world. Online safety risks are posed more by behaviours and values than the technology itself.

2.1.2 Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies which detail how new and emerging technologies may be used.

2.1.3 Communication with pupils both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries in line with Safer Working Practices.

2.1.4 Staff should not request or respond to any personal information from pupils other than which may be necessary in their professional role. They should ensure that their communications are open and

transparent and avoid any communication which could be interpreted as ‘grooming behaviour’.

2.1.5 Staff should not give their personal contact details to pupils for example, e-mail address, home or mobile telephone numbers, details of web based identities. If children locate these by any other means and attempt to contact or correspond with the staff member, the adult should not respond and must report the matter to the Headteacher. The pupil should be firmly and politely informed that this is not acceptable.

2.1.6 Staff should, in any communication with pupil, also follow the guidance in section 7 ‘Standards of Behaviour’ of ‘Guidance for safer working practice for those working with children and young people in education settings (October 2015)’.

2.1.7 Staff should adhere to their establishment’s policies, including those with regard to communication with parents and carers and the information they share when using the internet.

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 code of conduct. 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 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 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.

2.2.4 All schools should have their own internal Acceptable Use Policy.

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 undermine their professional position if they are published outside of the site.

2.3.4 Staff should not seek to communicate/make contact or respond to contact with pupils outside of the purposes of their work.

2.3.5 Staff should not give out their personal details.

2.3.6 Staff should use only equipment and Internet services provided by the school or setting.

2.3.7 Staff should follow their school/setting's Acceptable Use policy.

2.3.8 Staff should ensure that their use of technologies could not bring their employer into disrepute.

2.3.9 Confidentiality needs to be considered at all times. Social media has 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.

2.3.10 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 media (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, or Bath and North East Somerset Council could result in formal action being taken against them.

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

2.3.12 Adults within the school setting must never post derogatory remarks or offensive comments on-line or engage in online activities which may bring the school or Bath or North East Somerset Council into disrepute or could reflect negatively on their professionalism.

2.3.13 Some social media sites and other web-based sites have fields in the user profile for job title etc. If you are an employee of a school and particularly if you are a teacher/teaching assistant, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school, the profession or the Local Authority.

Update: With respect to PREVENT, all concerns regarding school or non school ICT equipment being used onsite or offsite to access, or distribute, materials related to terrorism should be reported to the Head Teacher immediately.

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. Where there is a need for homework to be sent electronically the school e-mail address should be used.

2.4.4 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.

Adults working in schools should ***not***:

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

2.4.7 Use their own mobile phones to contact pupils or parents.

2.5 Communication between pupils / adults working in school

2.5.1 The school normally provides a work mobile and e-mail address for communication between staff and pupils where this is necessary for particular trips/assignments. Adults should not give their personal mobile numbers or personal e-mail addresses to pupils or parents for these purposes.

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.

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. Internal e-mail systems should only be used in accordance with the school'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 pupils or parents.

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 or are related. 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.

2.6.3 There must be awareness on the part of those working with or in contact with pupils 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 Staff should not establish or seek contact via a social networking site with any current or ex pupils under 18 years old. Any contact with any adult ex pupils should be openly acknowledged as to the reason for the social link i.e. friend of family or work colleague.

2.6.5 Staff should always inform the head teacher or DSL of any pupils attempting to make contact via social media i.e. Instagram. Parents of that child will be informed and this will be logged in our 'Online Safety' log.

2.6.6 Staff should not include their place of work on any social networking profile as is recommended good practice. Staff should check their privacy settings regularly on social media to reduce the likelihood of pupils, ex pupils and parents accessing personal information.

2.6.7 Staff must never mention or comment on individual children within any context either in school or out e.g. school residential. Staff must be mindful the negative or ambiguous posts about school which could bring staff, pupils or and parents into disrepute. With our new Twitter account staff will be encouraged to use this as a safer and more appropriate platform to celebrate pupils success e.g. a spring concert.

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 downloaded images 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 has 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 refer to the dealing with allegations of abuse against adults policy and should not attempt to investigate or evaluate the material themselves until such advice is received.

2.8 Online bullying

2.8.1 Online 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 online bullying. All adults are reminded of the need to protect themselves from the potential threat of online bullying.

Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

2.8.3 If online 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. Employees will also have access to the Health Assured Employee Assistance Programme, telephone 0800 030 5182, a free 24 hour confidential counselling and advisory service, (subject to appropriate funding arrangements)

2.8.5 Adults are encouraged to report all incidents of online bullying to their line manager or 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:

- Keeping Children Safe in Education 2016
- IT policy
- Disciplinary policy and procedures
- Equal opportunity policy
- Code of conduct
- Guidance for Safer Working Practice for Adults who Work with Children and Young People 2015

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.

Date for review: June 2018

Appendix A – Relevant legislation

School staff 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
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). A person convicted of such an offence may face up to 10 years in prison.

Sexual offences act 2003
The new 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, connexions staff 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. Children, Families and Education Directorate page 38 April 2007.

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 school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.