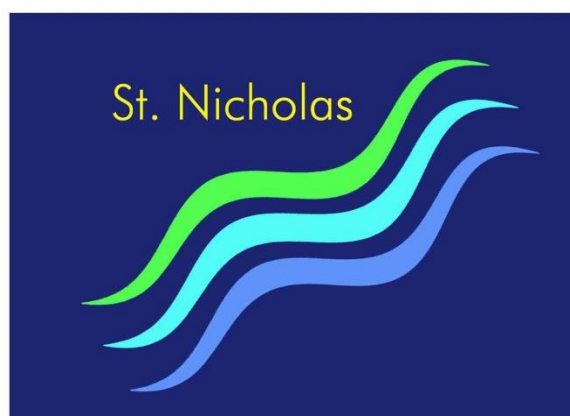# Social Media Policy

St Nicholas CE Primary School

Approved by:	St Nicholas CE Primary School Governing Body	Date: August 2016
Last reviewed on:	25th April 2018	
Next review due by:	April 2019	

Section 1: Introduction

1.1   Objectives

1.1.1   This policy sets out St Nicholas CE 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 St Nicholas CE 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 Headteacher 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.

1.2   Scope

1.2.1   This document applies to all adults who work in St Nicholas CE 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 their manager. 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   The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

2.2.2   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.

2.2.3   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.

2.2.4   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.

2.2.5   All members of the school community are expected to engage in social media in a positive, safe and responsible manner, at all times.

2.2.6   All members of the school community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

2.2.7   The school will control pupil and staff access to social media whilst using school provided devices and systems on site.

2.2.8   The use of social media during school hours for personal use by staff is permitted during their breaks.

2.2.9   Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.

2.2.10   Concerns regarding the online conduct of any member of school community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Safeguarding policies.

2.3   Staff personal Use of Social Media

2.3.1   The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

2.3.2   Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of conduct within the AUP.

2.4 Protection of personal information

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

2.4.2   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.

2.4.3   Adults working in schools should:

- Never share their work log-ins or passwords with other people.
- Keep their personal phone numbers private
- 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.
- 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.
- Only equipment and Internet services provided by the school or setting.
- Follow their school/setting's Acceptable Use policy.
- Ensure that their use of technologies could not bring their employer into disrepute.
- Ensure that confidentiality is 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.
- 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.
- Remember that they must comply with the requirements of equalities legislation in their on-line communications.

2.4.4   Adults working in schools should *not*:
- Use school ICT equipment for personal use, e.g. camera or computers.
- Use their own mobile phones to contact pupils or parents except in exceptional circumstances when they should withhold their number.

- 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.
- 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.

2.4.5   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.

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

2.5 Reputation

2.5.1   All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

2.5.2   All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites as strictly as they can.
- Being aware of location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring staff do not represent their personal views as that of the school.

2.5.3   Members of staff are encouraged not to identify themselves as employees of St Nicholas CE Primary on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.

2.5.4   All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework.

2.5.5   Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.

2.5.6   Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

2.5   Communication between pupils / adults working in school

2.5.1   All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.

- Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the headteacher.

- If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.

2.5.2   Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.

2.5.3   Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

2.5.4   The school 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.

2.5.5   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.

2.5.6   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.

2.5.7   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.

2.5.8   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.

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

2.6 Pupils' Personal Use of Social Media

2.6.1   Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.

2.6.2   The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.

2.6.3   Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

2.6.4   Pupils will be advised, through the e-safety curriculum to:

- consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
- only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
- not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- use safe passwords.
- use social media sites which are appropriate for their age and abilities.
- block and report unwanted communications and report concerns both within school and externally.

2.7 Official Use of Social Media

2.7.1   St Nicholas CE Primary School's official social media channels are: **Facebook and Twitter**

2.7.2   The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.

2.7.3   The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.

2.7.4   Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence.

2.7.5   Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.

2.7.6   Staff use school provided email addresses to register for and manage any official school social media channels.

2.7.7   Official social media sites are suitably protected and, where possible, are linked to the school website.

2.7.8   Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.

2.7.9   Official social media use will be conducted in line with existing policies, including: Anti-bullying, GDPR, Confidentiality and Child protection.

2.7.10   All communication on official social media platforms will be clear, transparent and open to scrutiny.

2.7.11   Parents, carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

2.7.12   The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

2.8 Staff expectations when using School Social Media

2.8.1   Members of staff who follow and/or like the school social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

2.8.2   If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:

- Sign the school's Social media acceptable use policy.
- Be professional at all times and aware that they are an ambassador for the school.
- Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
- Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws.
- Ensure that they have appropriate written consent before posting images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
- Inform their line manager, the Designated Safeguarding Lead and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

2.9   Access to inappropriate images and internet usage

2.9.1   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.

2.9.2   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.

2.9.3   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.

2.9.4   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.

2.9.5   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.

2.10   Online bullying

2.10.1   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.'

2.10.2   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.

2.10.3   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.

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

2.10.5   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.

2.11   Parental use of social media

2.11.1   Parents and carers will be made aware of their responsibilities regarding their use of social networking.

2.11.2   Methods of school communication include the prospectus, the website, newsletters, letters and verbal discussion. School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion. Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.

2.11.3   Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event.

2.11.4   Parents should make complaints through official school channels rather than posting them on social networking sites.

2.11.5   Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

2.12   Dealing with incidents of online bullying/inappropriate use of social networking sites

2.12.1   The school's Anti-Bullying Policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll.

2.12.2   In the case of inappropriate use of social networking by parents, the Governing Body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy and will send a letter.

2.12.3 The Governing Body understands that there are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged. Furthermore, laws of defamation and privacy still apply to the web and it is unlawful for statements to be written which:

- expose (an individual) to hatred, ridicule or contempt
- cause (an individual) to be shunned or avoided
- lower (an individual's) standing in the estimation of right-thinking members of society or
- disparage (an individual in their) business, trade, office or profession." (National Association of Headteachers)

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
- Safeguarding Policy
- Online Safety 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.

Section 4: Monitoring Arrangements

4.1.1 This policy will be reviewed yearly or as appropriate by the Computing subject leader and the Senior Leadership Team. (SLT) At every review, the policy will be shared with the governing board.

This policy was adopted by the Governing Body: May 2018

Signature of Chair of Governing Body:

Next Review Date: September 2018 (or earlier due to change in statutory guidance/internal review)