School: Bentilee Nursery school	
Date Adopted: 2/3/23	

City of
Stoke-on-Trent

Social Networking Protocol

for

Schools & Academies

Author	Schools HR Business Management	Address	Floor 2 Civic Centre Stoke on Trent
Document	Social Networking Protocol		
Date Created	January 2023		.
	Next review- Sept 25		

N.B For the purposes of clarity, references to;

- Governing Body may mean Board of Directors or Academy Committee
- Governors may mean Directors and/or Local Academy Representatives (In accordance with the relevant Scheme of Delegation of Authority).

Review	1	2	3	4	5	6	7	8
Date	Sept 2018	Sept 2024						

Social Networking Protocol

Contents

Do not use social networking sites or online blogs to make comments on anything related to the school: its activities, its pupils, parents, partners, governors or colleagues. It is recommended that employees do not state their current place of work on any of their profiles.

1. Purpose

1.1. Over recent years there has been an increase in the availability and use of internet sites for social networking and communication. These websites make it easy to keep in touch informally with friends, share news, arrange events and express views and opinions; often people use it to conduct their social lives online and make new friends. Others use networking sites for formal professional means to share contacts, ideas and best practice.

1.2. Some examples of networking sites include Twitter, Facebook, Instagram, LinkedIn, YouTube, TES forums, Whatsapp and Snapchat Blogs are also included under this protocol as are any new sites which may emerge after the creation of this protocol.

1.3. This protocol is designed to inform employees of expected professional standards and to alert them of the potential problems that may arise in the use of social networking sites.

1.4. Whilst an employee's right to privacy is respected, employees have a duty to their employer and to their colleagues to maintain professional standards, not only during working hours but also outside of work if what they do, say or write may have an impact on their workplace.

1.5. This protocol recognises the guidance set out in the document 'Guidance for Safer Working Practice for Adults who work with Children and Young People' (Staffordshire and Stoke on Trent Safeguarding Children Boards).

2. Scope

2.1. This protocol applies to all academy and maintained school employees.

3 Principles

3.1 An employee has the right to a private life but it must not adversely impact on their place of employment.

3.2 The school/academies E-Safety Policy makes clear what acceptable internet use is when employees are at work and access to most networking sites is restricted during work time. All employees must be fully informed of the school's E-Safety policy and what is deemed to be acceptable usage of school equipment and internet services.

3.3 It is advisable that all employees demonstrate online awareness and take precautions to avoid leaving themselves vulnerable to allegations relating to the posting of comments and other material online. (Appendix 1)

3.4 This protocol may be used in conjunction with other school policies to address online abuse such as inappropriate activities, obscenity, harassment and any form of discrimination or unwanted behaviour towards colleagues, pupils, their families and other members of the school/academy community

3.5 The school's Code of Conduct, Confidential Reporting (whistleblowing), E-Safety policies, GDPR and Equal Opportunities policy may also set out guidance for online activity (this list is not exhaustive).

3.6 Whilst employees use differing social networks, with this comes the increased security risks of data being lost, corrupted or misused. An employee must ensure that they comply with GDPR when using any internet based system as the use of such systems pose risks to privacy and data security.

4 School's Expectations

4.1 The pupils, parents, colleagues and school governors/academy representatives are entitled to expect the highest standards of conduct and professionalism including participation on social networking sites from all employees who work at the school/academy.

4.2 An employee who is subject to threats, abuse or harassment via social networking sites from a work colleague, pupil, a member of the pupil's family or other relevant person, should report the incidents to the Headteacher/Principal immediately.

5 Safeguarding

5.1. Care should always be taken to maintain appropriate personal and professional boundaries when participating on social networking sites. School employees should not accept online friend requests from pupils or their families, unless there is good reason for this contact and it has been agreed in advance with the Headteacher/Principal. In these circumstances the information shared online with the pupil or their families must be appropriate to the professional role and all communication must be transparent and open to scrutiny.

5.2. If a pupil, parent or other family member seeks to establish online contact, or contact occurs coincidentally, school employees should not share any personal information, nor should they request or respond to personal information from the pupil or family member. Employees should exercise their professional judgement in dealing with the situation. The incident should be recorded and discussed with the Headteacher/Principal or line manager. If

appropriate, the matter should also be discussed with the parent of the child or young person before proceeding further.

5.3.   There may be occasions when social networking sites are accessed through the school's IT systems for work related reasons. Use of these sites during work time is prohibited, unless permission for a work purpose has been granted in writing by the Headteacher/Principal or Line Manager. If permission has been granted by the Headteacher/Principal for a school employee to access social networking sites for a work related purpose, this should only be done using devices belonging to the school, and not from the employee's own personal device.

5.4.   School employees using social networking sites to make approved contact with a pupil or student as outlined in section 5.3, should keep a log of any communication. Staff should take extreme care of the content of their communications with pupils so as to avoid any possible misinterpretation of their motives or behaviour. Only employees who have been granted permission should post on the school's networking site

5.5.   If school employees are to make contact with pupils or students via social networking sites, consent must be obtained from the parent or carer if the pupil is under 16. It is also recommended that for young people over 16, their parents/carer are also informed of the intention to communicate via social networking sites and the reason for doing so clearly explained.

5.6.   Once the reason for accessing social networking sites has ended, any online relationships with pupils or students should cease immediately. Employees should not continue to develop and maintain online relationships via social networking sites with pupils or students they work with or have previously worked with. Once all communication has ended the method of contact should be deleted e.g. deletion of friend status on Facebook, to ensure no further communication can be made.

5.7.   If employees are in any doubt as to what is permissible and what their personal responsibilities are they must seek guidance from the Headteacher/Principal.

6.   **Privacy**

Employees must ensure that their account settings do not compromise their professional position. This can be done by applying the correct privacy setting. It is recommended that the following are set:

- Your status, photos and posts – friends only
- Photos and videos you you're tagged in – friends only
- Contact information – friends only

Employees should ensure that they use secure networks when accessing internet sites and that privacy settings are set appropriately for all social networking platforms.

7.   Monitoring

7.1.   The school will investigate misconduct or complaints brought to its attention and may use information available on internet sites for this purpose. This may include information from employees' personal social networking sites, reviewing e-mails or examining accessible internet logs. Employees who wish to send confidential personal e-mails should not use the school's e-mail addresses or computer system.

8   Disciplinary Action

8.1.   Employees should not post or 'like' any material that is harmful to the reputation of colleagues or the school, for example derogatory, false, misleading, threatening or lewd posts, comments or images.

8.2.   Online activity which is deemed to be in contravention of section 7.1 will be subject to the schools disciplinary policy.

8.3.   If employees are suspected of participating in inappropriate conduct in breach of this protocol, (including online activity which takes place outside of normal working hours) an investigation may be carried out under the schools disciplinary procedure. In the case of gross misconduct this could result in dismissal.

8.4.   An investigation into an employee's conduct online may lead to the content of the employee's social networking site being reported to the relevant body or authority including the Police.

8.5.   Such conduct could arise from the following:

- Posts, comments or material (including "liking" posts, comments or material) which amount to a form of grooming, serious harassment, obscenity, bullying or intimidation, abuse, defamation or any breach of discrimination legislation etc.

- Online interaction with children or parents outside of the working relationship which is deemed to be in breach of this protocol and inappropriate in accordance to LA and safeguarding policies.

- Improper disclosure of information, breach of privacy, copyright or data protection.

- Online activity which can be shown to have caused damage to the reputation of the school, and/or can also be shown to be malicious and unjustified.

- Commentary, content, recordings or images that may be considered to be defamatory/libellous, pornographic, improper or that can create a hostile work environment or which represents or creates a threat to the health and safety of colleagues and students or which is considered generally offensive.

N.B. this list is not exhaustive

Appendix 1

Online awareness

Employees are reminded of the following points:

1) They are legally liable for anything posted online.

2) It is strongly recommended that employees do not post any personal information online such as address, date of birth or financial details, in order to protect their identity.

3) Messages should not be regarded as private if security settings are not set correctly. If messages are to be posted which are not intended for public viewing, the settings should be adjusted so all content is private to the selected group of people. For example on Facebook, the "friends only" setting ensures the audience is limited and access to the personal profile is controlled.

4) Employees should be aware of the nature of the photographs they upload onto social networking sites and consider whether they are appropriate in relation to their professional role. This includes other users posting a photo of the employee which may lead to comments being posted in a wider arena. Employees should be aware that they can be 'tagged' in a photo, and the photo can then be uploaded onto the site without the individual's permission. If this occurs and the photo and / or subsequent comments are inappropriate, the employee should request that the material is removed by the user who posted the initial image.

5) If employees do not wish work colleagues to see their posts, they should not be added as friends.

6) Employees should not give people who are not known to them access to their information. The employee may without realising, be giving access to their personal profile and web pages to people who may know the employee or who are looking for information connected with the employee or the school.

7) Even though employees may not directly identify names of colleagues or the school as the employer, people accessing sites may be aware of where employees work and will therefore link any comments and views, expressed about work or otherwise, with the school and its employees.

8) The internet is a widely used public forum, and when statements or posts are made on websites they can be irreversible and are subject to the same liable legislation as other forms of written media.

9) Even restricted settings do not guarantee a post or comment will not be circulated to, or read by someone who was not intended to see it; and who may take offence at the contents despite not having direct access to the information.

10) The usual signs that help employees avoid offence such as body language are not available online, and it is easy to make 'throwaway' comments in jest which may be misinterpreted, taken seriously and considered offensive.

11) Copyright laws still apply online. Do not use images to which you do not hold the copyright. Information shared should be attributed to the source.

12) Employees should be aware that even if a social media post is deleted a copy may have been retained, or it may have been cached on the internet.

13) Employees may choose to use a pseudonym for social accounts, in which case Section 6 of the policy relating to privacy setting will still apply.

Responsibilities as an employee of the school

Posting information into a public area has the potential of directly/indirectly impacting on the workplace. Employees publishing comments on any site or in any forum to which members of the public may have access should be careful to abide by the following rules:

1) Employees should ensure that online activities do not bring the school into disrepute or adversely affect the employee's position within the school.

2) Employees must not make derogatory comments about the school, or past and present colleagues which may damage the school's reputation and / or the individual's.

3) Whilst people may seek to use these sites to 'let off steam' employees must avoid saying anything in the heat of the moment or make complaints, which may undermine the school's decisions and create a poor impression of the school's principles, standards and work undertaken by the school.

4) Employees must not make statements which may have a negative or damaging effect on working relationships.

5) Employees should not engage in any online communication with colleagues, pupils, their families or other relevant person, which may amount to bullying and harassment, Nor should employees make unwanted or unwelcome online communications to those who do not wish to receive them. This includes posting comments about colleagues, pupils or their families in public forums to which they, their friends, family, neighbours or colleagues might have access.

6) Employees should not post gossip or circulate rumours about the school or past or present colleagues, as this will almost always adversely affect the impression of the school, as well as damaging the reputation of individuals and the school.

7) Any information which is posted online should not contradict information provided formally by the school or contradict the effect of a policy in force at the school.

8) Employees should make it clear that any views expressed are their own and do not reflect the views of the school, the post should not identify the employee as a representative of the school expressing views which are related to work.

9) The school values diversity and has pupils and staff from a wide range of backgrounds. Employees should not post offensive or discriminatory remarks which may lead to concern with regard to the suitability of the post-holder, as they are required to behave in a manner compatible with the School's equal opportunities policies. Employees should also not post material that may lead to concern regarding

the ability of the employee to commit to the schools expectations, standards and policies.

10) Employees should be careful not to join or be associated with online groups which, due to their content or objectives, are incompatible with the policies and objectives of the school.

11) Confidential information about the school should not be posted. This may include aspects of school policy or details of internal discussions about work or colleagues.

12) Employees' email address or work numbers should not be included on personal online profiles or otherwise posted online.

13) Privacy of colleagues and pupils should be maintained at all times.