Social Networking Protocol

Date of Policy	2022
Reviewed and Agreed by	The Directors’ Board
Review Date	14 July 2022
Next Review Date	Autumn 2024

Social Networking Protocol

Contents

Do not use social networking sites or online blogs to make comments on anything related to The Societas Trust, its academies, its activities, its pupils, parents, partners, governors or colleagues.

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, Friendster, LinkedIn, YouTube and My Space. 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 The Societas Trust (The Trust) 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' September 2019 (Staffordshire and Stoke on Trent Safeguarding Children Boards).

2 Scope

2.1 The protocol applies to all Trust employees, governors, agency workers, volunteers or those engaged in consultancy work (herein referred to generically as 'employees').

3 Principles

3.1 The right to a private life is respected by the Trust provided it does not adversely impact on the activities of the Trust or its academies.

3.2 The Trust's Information Security Policy makes it clear what is acceptable internet use when employees are at work; access to most networking sites is restricted so access is prevented during work time. All employees must be fully informed of this policy and what is deemed to be acceptable usage of Trust / Academy 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 Trust / Academy 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 community.

3.5 The Trust's Code of Conduct, Confidential Reporting, Information Security, Data Protection and Equal Opportunities policies may also set out guidance for online activity (this list is not exhaustive).

3.6 The protocol has been consulted upon with recognised Teaching and Support Staff Trade Unions.

4 Expectations

4.1 The pupils, parents, carers, colleagues and governors are entitled to expect the highest standards of conduct and professionalism from all those who work for the Trust, including participation on social networking sites.

4.2 Anyone subject to threats, abuse or harassment via their use of social networking sites whilst working on behalf of the Trust should report the incidents to their Head Teacher / Manager immediately.

4.3 Anyone working on behalf of the Trust who is subjected to threats, abuse or harassment via social networking sites from a colleague, pupil, member of the pupil's family or other relevant person, should report the incidents to the Head Teacher / Manager immediately.

5 Safeguarding

5.1 Care should always be taken to maintain appropriate personal and professional boundaries when participating on social networking sites. 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 Head Teacher / Manager. 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, 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 Head Teacher 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 academy 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 Head Teacher / Manager. If permission has been granted by the Head Teacher / Manager for an employee to access social networking sites for a work related purpose, this should only be done using devices belonging to the Trust / Academy, and not from the employee's own personal devices.

5.4 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. Employees 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 Trust's / Academy's networking site

5.5 If 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 are also informed of the intention to communicate with their child 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 Head Teacher / Manager.

6 Monitoring

6.1 The Trust will monitor on-line activity on all Trust and Academy IT equipment and 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 their work e-mail addresses or computer system.

7 Disciplinary Action

7.1 Employees should not post or ‘like’ any material that is harmful to the reputation of colleagues, the Trust, or the Academy: this would include derogatory, false, misleading, threatening or lewd posts, comments or images.

7.2 Online activity which is deemed to be in contravention of section 7.1 will be subject to the Trust’s disciplinary policy.

7.3 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 Trust’s disciplinary procedure. In the case of gross misconduct this could result in dismissal.

7.4 An investigation into an employee’s conduct online may lead to the content of the employee’s social networking site being reported to a relevant body or authority.

7.5 Such conduct could arise from the following (this list is not exhaustive):

- 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 with safeguarding practices and 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 Trust or Academy, 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.

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 Trust / Academy.

7) Even though employees may not directly identify names of colleagues or the Trust 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 Trust 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.

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.

Appendix 2

Responsibilities as an employee of the Trust / Academy

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 Trust / Academy into disrepute or adversely affect the employee's position within the Trust / Academy.

2) Employees must not make derogatory comments about the Trust / Academy, or past and present colleagues which may damage the Trust's / Academy'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 Trust's / Academy's decisions and create a poor impression of the Trust's / Academy's principles, standards and work undertaken by the Trust / Academy.

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 Trust / Academy or past or present colleagues, as this will almost always adversely affect the impression of the Trust / Academy, as well as damaging the reputation of individuals and the Trust / Academy.

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

8) Employees should make it clear that any views expressed are their own and do not reflect the views of the Trust / Academy, the post should not identify

the employee as a representative of the Trust / Academy expressing views which are related to work.

9) The Trust 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 Trust'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 Trust's 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 Trust / Academy.

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

12) Employee's 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.