Social Media Use. Policy and Guidelines

Key document details

Author:	DPO	**Approver:**	TB
Owner:	SRAT	**Version no.:**	1
Last review:	September 2022	**Next review:**	September 23
Ratified:			

The aim of this policy on social media is to provide a framework that the Steel River Academy Trust can adopt to enable employees to enjoy the benefits of social networking while understanding the standards of conduct expected by the Trust. It is intended to minimise the risks that can impact on the wellbeing of staff, pupils and the reputation of the trust.

Section 1: Introduction

Steel River Academy Trust recognised and embraces the numerous benefits and opportunities that social media offers. While employees are encouraged to engage, collaborate and innovate through social media, they should be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation

Section 2: Purpose of the Policy

2.1 The purpose of this policy is to encourage good practise, to protect the Trust and its employees, and to promote the effective use of social media as part of the trust's activities

2.2 The policy covers personal and professional use of social media and aims to encourage its safe use by the trust and its employees

2.3 The policy applies regardless of whether social media is accessed using the trust's ICT facilities and equipment, or equipment belonging to members of staff

2.4 Personal communication via social media accounts that are likely to have a negative impact on professional standards or the Trust's reputation are within the scope of this policy

2.5 This policy covers all individuals working at all levels and grades, including full-time and part-time employees, fixed-term employees and agency workers.

Section 3: Roles, responsibilities and procedures

3.1: Employees should

- Be aware of their online reputation and recognise that their online activity can be seen by others including parents, pupils and colleagues on social media
- Ensure that any use of social media is carried out in line with this policy and other relevant policies
- Be responsible for their own words and actions in an online environment. They are therefore advised to consider whether any comment, photograph or video that they are about to post on a social networking site is something they want pupils, colleagues, other employees of the Trust, or even future employers, to read. **If in doubt, don't post it**

3.2 Managers are responsible for:

- Addressing any concerns and / or questions employees may have on the use of social media
- Operating within the boundaries of this policy and ensuring that all staff understand the standards of behaviour expected of them
- Implementing and reviewing this policy

Section 4: Definition of social media

4.1 Social media is a broad term for any kind of online platform which enables people to interact with each other. It allows people to share information, ideas and views. Examples of social media include Facebook, Twitter, LinkedIn, WhatsApp, Instagram, etc.

Section 5: Acceptable Use

5.1 Employees should be aware that content uploaded to social media is not private. Even if you restrict it to 'friends', there is still capacity for it to be reposted or distributed beyond the intended recipients. Therefore, employees using social media should conduct themselves with professionalism and respect

5.2 Employees should not upload any content on to social media sites that:

- Is confidential to the Trust or its staff
- Amounts to bullying
- Amounts to unlawful discrimination, harassment or victimisation
- Brings the Trust into disrepute
- Contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images or clips
- Undermines the reputation of the Trust, its schools and / or individuals
- Is defamatory or knowingly false
- Breaches copyright
- Is in any other way unlawful

5.3 Employees should be aware of both professional and social boundaries and should not therefore accept or invite 'friend' requests from pupils or ex-pupils under the age of 18, or from parents on their personal social media accounts such as Facebook. All communication with parents via social media should be through the Trust school's social media accounts.

5.4 Employees should note that the use of social media during lesson times is not permitted

5.5 Employees may legitimately access social media sites for work purposes via school IT systems where this forms part of their role or with prior approval from the Head Teacher.

Section 6: Safeguarding

6.1 The use of social networking sites introduces a range of potential safeguarding risks to children and young people

Potential risks can include, but are not limited to:

- Online bullying
- Grooming, exploitation or stalking
- Exposure to inappropriate material or hateful language
- Encouraging violent behaviour, self-harm or risk taking

In order to mitigate these risks there are steps you can take to promote safety on line:

- You should not use any information in an attempt to locate or meet a child. Ensure that any messages, photos or information comply with existing policies. Further information can be found in appendix A.

Section 7: Reporting safeguarding concerns

7.1 Any content or online activity which raises safeguarding concerns must be reported to the Designated Safeguarding Lead within the Trust's schools.

7.2 Any online concerns should be reported as soon as identified as urgent steps may need to be taken to safeguard the child.

7.3 With regard to personal safeguarding, you should report any harassment or abuse you receive online while using your work accounts.

Section 8: Reporting, responding and recording cyber bullying incidents

8.1 Staff should never engage in cyber bullying incidents. If in the course of your employments with the Steel River Academy Trust you discover a website containing inaccurate, inappropriate of inflammatory written material relating to you, or images of you which have been taken and / or which are being used without your permission, you should immediately report to a senior manager within your school

8.2 Staff should keep any records of abuse, such as text messages, emails, voicemail, website or social media. If appropriate, screen prints of messages or web pages could be taken and the time, date and address of the site / number the message is received from should be recorded

Section 9: Action by the employer: inappropriate use of social media

9.1 Following a report of inappropriate use of social media, the senior management will conduct a prompt investigation

9.2 If in the course of the investigation, it is found that a pupil submitted the material to the website, that pupil will be disciplined in line with the Trust's behaviour policy

9.3 The senior manager, where appropriate, will approach the website hosts to ensure the material is either amended or removed as a matter of urgency, i.e. within 24 hours. If the website requires the individual who is complaining to do so personally, the Trust will give their full support and assistance

9.4 Checks will be carried out to ensure that the requested amendments or removals are made. If the website(s) does not co-operate, the senior manager will contact the internet service provider (ISP) as the ISP has the ability to block access to certain sites and, in exceptional circumstances, can close down a website

9.5 If material is threatening and / or intimidating, senior management will, with the member of staff's consent, report the matter to the police

9.6 The member of staff will be offered full support and appropriate stress counselling

Section 10: Breaches of this policy

10.1 Any member of staff suspected of committing a breach of this policy (or if complaints are received about the unacceptable use of social networking that has potentially breached this policy) will be investigated in accordance with the Trust's bullying or disciplinary procedure. The member of staff will be expected to cooperate with the Trust's investigation which may involve

- Handing over relevant passwords and login details

- Printing a copy or obtaining a screenshot of alleged unacceptable content
- Determining that the responsibility or source of the content was in fact the member of staff

10.2 The seriousness of the breach will be considered including the nature of the content, how long the content remained visible on the social media site, the potential for recirculation by others and the impact on the Trust or the individual(s) concerned

10.3 Staff should be aware that actions online can be in breach of the harassment / IT / equality policies and any online breaches of these policies may also be treated as conduct issues accordance with the disciplinary procedure. Advice from HR can be sought where necessary, particularly where disciplinary procedures are being considered.

10.4 If the outcome of an investigation leads to disciplinary action, the consequences will be dealt with in accordance with the appropriate procedures. Serious breaches could result in the dismissal of the employee

10.5 Where conduct is considered unlawful, the Trust will report the matter to the police and other external agencies

Section 11: Monitoring and review

11.1 If the manager reasonably believes that an employee has breached this policy, from time to time the school will monitor or record communications that are sent or received from within the Trust's network

11.2 This policy will be reviewed on an annual basis and, in accordance with the following, on an as-and-when required basis:

- Legislative basis
- Good practice guidance
- Case law
- Significant incidents reported

11.3 This policy does not form any part of an employee's contract of employment and may also, after consultation with the trade unions, be amended from time to time by the Trust

Section 12: Legislation

12.1 Acceptable use of Social networking must comply with UK law. In applying this policy, the Trust will adhere to its rights, responsibilities and duties in accordance with the following:

- Regulation of Investigatory Powers Act 2000
- General Data Protection Regulations (GDPR) UK 2021
- The Human Rights Act 1998
- The Equality Act 2010
- The Defamation Act 2013

Section 13: Conclusion

13.1 The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media – the principles set out in this policy must be followed irrespective of the medium.

When using social media, staff should be aware of the potential impact on themselves and the employer, whether for work-related or personal use; whether during working hours or otherwise; or whether social media is accessed using the employer's equipment or using an employee's equipment.

Staff should use discretion and common sense when engaging in online communication. There are some general rules and best practice in Appendix A which staff may find helpful.

Appendix A

Responsible use of Social Media – Guidance for Staff

Remember that anything you post online is not really private. Below are some common sense guidelines and recommendations that staff are advised to follow to ensure responsible and safe use of social media.

- Employees must not access social networking sites for personal use via school IT systems or using school equipment.
- Do not add pupils as friends or contacts in your social media accounts
- Follow the Social Media Policy
- Always maintain professional boundaries. Do not engage in discussions with pupils online unless through official school accounts. If an employee receives messages on his/her social networking profile which they think could be from a pupil they must report this to the Headteacher, who will decide the appropriate action.
- Think about the potential risks; professional boundaries of adding parents to your personal social media accounts (refer to policy)
- Consider using an alternative name on sites like Facebook to make it harder for pupils to find you. For example, some staff use their first name and middle name rather than their surname, or their surname backwards
- Never post anything that is offensive or aggressive, even if you are very angry or upset. It can easily be taken out of context
- Remember that humour is relative, e.g. posting about a recent stag / hen event may be deemed as inappropriate. Likewise, a few 'light-hearted' images about colleagues or students may not be perceived as such by either the subject(s) of the humour or the employer. the guiding rule is: if in doubt, don't post it.
- 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/academy, could result in formal action being taken. This includes the uploading of photographs which might bring the school into disrepute.
- Make sure you regularly check or refresh your site page to ensure it is free of any inappropriate comments and / or images
- If you are tagged in something on social media that you feel is inappropriate, use the remove tag feature to untag yourself
- Be cautious when accepting 'friend requests' from people you do not really know. Simply being a friend of a friend does not mean that they should have access to your details and posts on social media
- Review your profile information and settings regularly to ensure that it is appropriate as it may be accessed by colleagues, pupils, parents or prospective employers
- Check your privacy and security settings regularly, and keep your date of birth, address and telephone number to yourself. Identity theft is a growing crime and this kind of information could be used to gain access to your bank or credit card account
- If you feel dissatisfied and wish to rant about teaching, politics and life in general, consider doing so anonymously, through a networking account or blog which cannot be attributed to you. Check that anything you do post in this cannot identify you, the Trust or any of its schools, pupil or parents.

- Ensure that any comments and / or images could not be deemed as defamatory or in breach of copyright legislation
- Never post any information which can be used to identify a pupil
- Do not use social media in any way to attack or abuse colleagues or air any other internal grievances
- Do not post derogatory, defamatory, offensive, harassing or discriminatory content
- Do not engage in any conduct (using personal insults / obscenities) which would not be acceptable in the workplace
- Do not use social media to undertake 'whistleblowing' – raise concerns through the proper channels which would entitle you to legal protection (Public Interest Disclosure Act 1998).