

LSEAT SOCIAL MEDIA POLICY

Responsible post holder	Director of Marketing and Communications and Group Safeguarding Lead
Approved by / on	Trust SLT September 2023
Next Review	September 2024

Contents

1. Introduction.....	4
2. Purpose and Aims.....	4
3. Scope.....	4
4. Unacceptable Content.....	5
5. Personal responsibility.....	6
6. Educational approaches.....	6
7. Monitoring and Privacy.....	7
8. Relationships between staff and students online.....	8
9. Trust-maintained social media sites.....	8
10 Requests for information.....	8
11. Legislation.....	8

1. Introduction

- 1.1 London South East Academies Trust encourage the safe and effective use of social media for staff, and where age appropriate, pupils. Social media is generally regarded as the interaction between people using website and internet applications to create, share and exchange content, ideas and opinions. The rise in social media has resulted in fundamental changes in the ways individuals, groups and organisations communicate.
- 1.2 Social media is currently one of the most popular uses of the internet and has many benefits; it allows users to communicate easily and immediately with people they wouldn't otherwise be able to communicate with. However, there are also risks associated with social media which must be recognised and considered.
- The classification of activity regarded as social media includes, but is not limited to:
 - Social networking (e.g. Facebook, LinkedIn, WhatsApp the Trust social media platform)
 - Blogs (e.g. Twitter)
 - Social photo and video sharing (e.g. YouTube, Flickr, Instagram)
 - Collaborative projects (e.g. Wikipedia, Wiki)
 - Virtual social worlds (e.g. Second Life)
 - Virtual game worlds (e.g. World of Warcraft)

2. Purpose and Aims

- This policy has been created to:
 - Protect pupils and staff from the potential risks of social media use
 - Provide guidance to pupils and staff using social media
 - Set out the general principles that pupils and staff should adhere to when using social media, for their own safety and the safety of others

3. Scope

- 3.1 This policy is applicable to all pupils (who are using age appropriate social media), teaching staff, support staff, managers, and Trustees who may be using social media / the internet to communicate:
- Content that identifies them as LSEAT employees or pupils
 - Content relating to others within the School/Trust

- Content created in connection with their Trust employment or school
- Content about the School/Trust

For the purposes of this policy, the term **'user'** applies to any individual who satisfies these criteria.

3.2 Social media sites have a varied age limit on creating a user account. This policy is referring to all children and young people accessing age-appropriate content and sites. If a pupil is accessing content/social media sites that is not considered age appropriate this should be referred to the DSL and assessed as a safeguarding concern under the Safeguarding Policy.

Social Media Site	Age Restrictions
Instagram	13 years old and up
Facebook	13 years old and up
TikTok	13 years old and up
Snapchat	13 years old and up
Youtube	13 years old and up
Whatsapp	16 years old and up
Twitter	13 years old and up

3.3 This policy applies equally to the use of social media using either Trust-issued devices or personal devices. Trust-issued devices include PCs, laptops, ipads, tablets and smartphones. The policy also applies equally to the use of social media on or off Trust premises. The location of the individual posting social media content does not matter. For example, unacceptable content uploaded from a home PC will be regarded in the same way as unacceptable content uploaded from a PC within the Trust.

3.4 This policy also applies to internal Trust IT systems which include a social networking aspect including, but not limited to, SharePoint, Helix Media Library and Office 365 applications.

3.5 Reasonable personal use of social media within scheduled breaks is permitted, as long as it does not interfere with work commitments and complies with this policy. Personal social media communications which do not in any way relate to the Trust are not within the scope of this policy.

3.6 All other London South East Academies Trust/ School policies also apply in the context of social media.

4. Unacceptable Content

4.1 It is expected that users will act in a responsible and ethical manner when using social media, always treating others with dignity and respect. Regardless of the privacy settings applied to each site, users should assume that any content posted on social media is publicly visible and permanent. Users should be aware that even if content is deleted, it may not be permanently removed. Each individual is personally liable and will be held accountable for the content that they post.

4.2 Unacceptable content includes, but is not limited to, content that is:

- Abusive
- Commercially sensitive
- Confidential
- Defamatory
- Discriminatory

- Fraudulent
- In violation of copyright laws
- Indecent
- Likely to be considered bullying or victimisation
- Likely to be considered harassment (related to protected characteristics)
- Likely to be considered offensive
- Likely to cause reputational damage
- Likely to identify an individual, without the permission of the individual
- Likely to promote violence or terrorism
- Malicious
- Misleading
- Obscene
- Offensive (for example, racially, religiously, sexually or politically)
- Pornographic
- Unlawful
- Raises a Safeguarding concern

4.3 Users must not attempt to access or use someone else's social media profile without their permission.

4.4 If users are found to be in breach of these guidelines, they may be subject to disciplinary action. Please see the relevant Disciplinary Policy for more information. In more serious cases, an individual may also be subject to civil or criminal legal proceedings. Social media must never be used in a way that breaches this or any other Trust Policy.

4.5 If pupils or staff users become aware that content of this nature has been posted by someone connected with the Trust, they should make a teacher or line manager as appropriate, aware as soon as possible. If users wish to make a formal complaint about Trust-related social media, they should follow the normal Complaints Procedure.

4.6 If any content is shared that raises a concern under safeguarding or is illegal, multi-agency partners (police/children's services) may be informed. Social media should not be used to directly message any safeguarding related concerns.

4.7 Any information that is posted or shared using an anonymous account, that through investigation identifies there is a high probability that it has been posted by a staff member or pupil (or information has been shared by them to aid another individual) this will be subject to this policy and potential disciplinary stages.

4.8 Permission from the Marketing and Communications department must be obtained before using Trust branding in any form of social media.

5. Personal responsibility

Pupils and staff should endeavour to keep themselves safe at all times when using social media. Information such as postal addresses, email addresses, telephone numbers and bank details should never be posted online. Users should also be wary of posting personal details, photographs or details of their current location on social media sites.

5.1 Unwanted contact can be made very easily via social media sites; users should be aware of this and not accept befriending invitations from strangers.

5.2 Similarly, users should be very wary of any contact through which the ability to make money is being offered. The user should not respond and should report the matter to the School/Trust.

- 5.3 If using a shared device, users should ensure that they have logged off all social media sites before shutting down the device.
- 5.4 Full use should be made of all privacy and security settings within the social media sites being used and advice provided by the Trust/School regarding this.
- 5.5 The Trust is committed to providing a learning environment that is free from bullying, harassment and victimisation for all pupils and staff. This applies to all forms of bullying, harassment and victimisation, including situations where social media is used. If users become aware that they, or others, are being bullied, harassed or victimised through social media, they should carry out the following steps:
- Do not respond directly to the comments
 - Retain the evidence
 - Report the situation immediately to a teacher or line manager
- 5.6 Pupils: Full definitions of bullying and harassment can be found in the school's Anti-Bullying Policy (or equivalent). Any examples of these behaviours taking place through social media will be dealt with through the school's Student Behaviour Policy (or equivalent).
- 5.7 Staff: Please refer to the Dignity at Work Policy and Code of Conduct. Any examples of these behaviours taking place through social media will be dealt with through the Staff Disciplinary Policy and Procedures and Safeguarding Policy and Procedures.

6. Educational approaches

- 6.1 Schools will offer guidance and support to its pupils and staff on safe use of the internet and social media through (list not exhaustive and each school will implement an online safety curriculum relevant to school):
- School assemblies
 - RSHE lessons
 - Parent meetings and communication to parents
 - Enrichment opportunities (for example, displays, presentations, theme weeks, etc)
 - Via curriculum content when naturally occurring opportunities to do so arise
- 6.2 The Trust recognises that this is a rapidly and continually changing area of concern in which younger pupils are 'digital natives' and the staff advising them are not. It is therefore important that awareness raising opportunities are regularly available to staff so that they remain confident in their ability to appropriately advise pupils.
- 6.3 Age-appropriate guidance for pupils should include:
- Advice on personal responsibility
 - Specific guidance for female pupils who may be particularly susceptible to the risks of internet and social media use, for example, being approached (virtually or in person) by other users.
 - Providing strategies designed to improve resilience in the face of online abuse and how to respond and share concerns.
 - Advice, through curriculum and careers content, on how inappropriate use of social media can impact adversely on future career prospects.
 - Guidance on the law surrounding social media use, what is legal / illegal and the consequences of illegal activity.
 - Social media should not be used to directly message any safeguarding related concerns.
- 6.4 Instances of inappropriate use of social media may involve the Trust/School but take place beyond its direct control, for instance, at home, whilst travelling to / from School, etc. It is therefore important that the School should also seek to raise the awareness of

parents and involve them in the guidance and education processes surrounding this issue.

- 6.5 The concerns around inappropriate use should not be permitted to inhibit the deployment of social media, and more generally the internet, as an educational tool (age-appropriate access). This should be encouraged as a demonstration of how social media can and should have positive outcomes.

7. Monitoring and Privacy

- 7.1 Users should be aware that the Trust reserves the right to monitor and review all aspects of the use of the Trust IT network, including via wifi, and to keep logs of individual user activity, including use of social media sites. The user concerned will not necessarily be notified that monitoring and review is taking place.
- 7.2 User data will normally be treated as confidential and private. However, an investigation may take place under the following circumstances:
- Requests for access / monitoring from Police or Security Services, as allowed by current legislation
 - Requests made under the Data Protection Act (1998) or Freedom of Information Act 2000 (Scotland 2002)
 - Requests to establish facts as part of a misconduct investigation
 - Requests from the employee themselves
 - To facilitate the operation, repair and essential maintenance of Trust systems
 - Routine monitoring of network traffic and data stored on Trust systems as required by the Prevent and Safeguarding strategies.
- 7.3 For this reason, users should not use Trust IT resources for any purpose they would not wish to become known to the organisation.
- 7.4 Please refer to the IT Acceptable Use Policy for full details of monitoring and privacy in relation to the Trust IT and communication systems.

8. Relationships between staff and pupils online

- 8.1 Staff and pupils must not make or accept invitations to be friends, or form similar connections on social media sites, unless there is a legitimate Trust business reason to do so and this must be approved by the Head of School/ Headteacher prior to accepting invitation. Staff must at all times observe the boundaries of the professional staff/pupil relationship. It is strongly recommended that members of staff create separate professional and personal social networking profiles if using social media in this way.

9 Trust-maintained social media sites

- 9.1 The Trust maintains official accounts for social media sites such as Facebook, Twitter, Instagram and LinkedIn. These sites are monitored by the Marketing department and are the preferred accounts for users to communicate and interact with the Trust.
- 9.2 Responsibility for the suitability of information posted on Trust-maintained social media sites lies with the author, who must ensure that the material is appropriate for all users who might access it, including pupils under the age of 18. The Trust will remove any content found to be inappropriate and may block users from posting on these sites if it becomes necessary.

- 9.3 If users become aware of inappropriate material being posted outside normal working hours, they should report this to the site provider. Users should familiarise themselves with the terms and conditions of any social media site they are using.
- 9.4 If staff or pupils wish to set up a social media profile affiliated with the Trust/School, for example using the Trust/School name or branding, they must first obtain permission from the Director of Marketing and Communications and the relevant Head of School/Headteacher.

10 Requests for information

Users should not respond to requests for information from any external media outlet. Any contact made through social media from external sources regarding information relating to the School/Trust should be referred to the Director of Marketing and Communications.

11 Legislation

All social media use must comply with existing UK legislation and EU directives. Some of the main laws covering use/misuse of social media are (NSPCC, May 18):

Sexual Offences Act 2003

Includes the offence of sexual grooming. But action can only be taken by authorities where it can be proved an adult intended to meet a child. Increasingly, online abusers have no intention of meeting the child physically. They may, for example, persuade a child to perform sexual acts via a webcam.

Malicious Communications Act 1988

Makes it an offence to send a communication with the intention of causing distress or anxiety. But the intent to cause distress or anxiety can be difficult to prove because online groomers do the opposite to this. They may find out a child's interests from their online profile and use these to send messages aiming to build a rapport with the child they've targeted.

Communications Act 2003 Section 127

Section 127 makes it an offence to send an electronic message that is grossly offensive or of an indecent, obscene or menacing character. An online groomer may not be covered by this law because they may send messages that aim to build up trust with a child.

12 Further information and support available at

[UK Safer Internet Centre](#)

[NSPCC: Social Media](#)