



Social Media Policy

GDPR LA POLICY

Review: Annually

Next Review Date: May 2022

Role	Name
Headteacher	Caroline Rodgers
Chair of Governors	Linda Mosley
Designated Governor	Linda Mosley – GDPR Governor
Designated Senior Lead	Caroline Rodgers - Headteacher Jayne Saxton – SBO

This document will be reviewed annually and sooner when significant changes are made to the law

Contents

5.1 Introduction	Error! Bookmark not defined.
5.2 Scope and Responsibilities	Error! Bookmark not defined.
5.3 Social Media Standards	Error! Bookmark not defined.
5.4 Safeguarding and Reporting	4
5.4.1 Social media risks	4
5.4.2 Incident Handling	4
5.4.3. Incident Recording	5
5.5 Relevant Legislation	5
5.6 Breaches of this policy	5
Annex A	6

5.1 Introduction

- We recognise the benefits of social media, but it also brings potential risk, to the school and to individuals. For the purposes of this policy, 'social media' is defined as websites and applications (apps) that allow people to create or share content and/or participate in social networking. Examples include, but are not limited to, Facebook, Twitter, LinkedIn, Instagram, Snapchat, Reddit, Pinterest, YouTube, WordPress, Tumblr, Ask.fm, WhatsApp.
- We realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin board to share good practice and disseminate information and resources. The use of online discussion groups and bulletin boards relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.
- This policy requires social media users to act responsibly and professionally and use social media in a way that minimises the associated risks, such as reputational damage, supports safeguarding and complies with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018) and best practice.

5.2 Scope and Responsibilities

All staff and volunteers, including Governors, are expected to comply with this policy.

External support providers and those acting under contractual obligation are expected to support this policy.

This policy applies to all use of social media including;

- Work-related use or personal use
- During working hours or out of hours
- On-site or off-site
- Through the school's internet network or otherwise
- On school owned or personal devices
- On official school social media accounts/platforms or personal accounts/platforms

In order to be an official 'school platform':

- Master privileges and access permissions are to be held by the school
- The school must have editorial oversight of all content
- The number of staff members with administrative rights should be limited to those necessary

Accounts are not school platforms unless the above conditions are met, regardless of whether account names may infer it. The school will not accept liability for content and postings on accounts containing the school name which have not been authorised and do not meet the above 'school platform' criteria.

Platforms used must be listed in the Privacy Notice, and personal information and pictures must not be posted without appropriate consent and oversight. Authorised accounts will remain the property of the

school and may be deleted at any time by the school. A log of such will be kept (see Annex A for proforma log)

5.3 Our Social Media Standards

Employees should:

- Be aware of their online reputation and digital footprint and recognise that their online presence and activities may be visible to the wider school community, including parents, pupils and colleagues.
- Protect confidentiality and ensure that their use of social media complies with legislation and is carried out in accordance with this policy.
- Be responsible for verifying the factual content of any posts or messages and ensure professional language is used at all times.
- Be aware that the person they are 'talking to' may not be disclosing their real identity. It is very easy to hide an identity in an on-line conversation.
- Be responsible for checking images and/or videos shared via digital media platforms are covered by the appropriate consent and ensure they are aware of the process for removing posts if consent is withdrawn.
- Be aware that posts, once shared, may be screenshot or distributed beyond the intended audience, despite post privacy settings.
- Be transparent about their role, especially when representing the school in an official capacity.
- Ensure that any personal opinions are made clear and clearly distinct from their role in school.
- Only use official school platforms to post school information, celebration, news and photographs.
- Ensure all posts are in line with the Safeguarding Policy and have appropriate privacy settings.
- Only communicate with current and ex-pupils in ways which may be considered appropriate, and avoid any words or actions which may breach the adult-pupil relationship of trust.
- Do not befriend or add current pupils to personal accounts, unless there is a familial connection to them and maintain professional boundaries.
- Do not discuss school matters, child progress or issues via social media.
- Report any inappropriate contact from pupils to [a member of SLT] at the earliest opportunity to prevent situations from escalating.
- Refer any safeguarding concerns to the DSL via the usual school channels and as soon as you identify them.

Managers should:

- Be the first point of contact for employees with queries surrounding social media and refer these on or signpost as appropriate.
- Have oversight of posts
- Periodically monitor communications which are sent/received from official school platforms

- Monitor and review user access to official school platforms.

In the event of an incident affecting the school or any members of the school community only official communications channels and accounts should comment or share news or updates.

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

- Is confidential to the school/trust or its staff
- Amounts to unlawful discrimination, harassment or victimisation or bullying
- Brings the school into disrepute and threatens the reputation of the school or staff
- Is defamatory or knowingly false
- Breaches copyright

5.4 Safeguarding and Reporting

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

5.4.1 Social media risks

Potential risks to pupils 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.

Staff can also be subject to allegations of abuse, misconduct or inappropriate behaviour.

5.4.2 Incident Handling

Individuals should not attempt to investigate cyberbullying incidents or try to access websites which have been reported to them as inappropriate, without suitable training. All incidents should be reported to the DSL / Headteacher as the earliest opportunity.

Designated staff should keep any records of alleged abuse, such as text, emails, voicemail, website or screenshots of social media posts, with the time and date. Web addresses of any related sites should be recorded.

If necessary, website hosts / platform providers will be contacted to request that content is amended or removed. If hosts or providers require an account holder to make a complaint, the school will support and assist, where possible.

The DSL will consider whether a [CEOP Report](#) is necessary and action this, if appropriate.

If, during the course of any investigation, it is found that a pupil submitted inappropriate material or is proven to have acted maliciously or illegally, that pupil will be disciplined in line with the school's behaviour policy.

If, during the course of any investigation, it is found that an employee submitted inappropriate material or is proven to have acted maliciously or illegally, that individual will be subject to the school's disciplinary procedures.

In cases where material is threatening and/or intimidating, or where illegal activity is suspected, information, including records of computer access, screenshots and messages, may be shared with the police.

5.4.3. Incident Recording

Concerns and complaints relating to social media activity or account should be directed to a member of SLT.

5.5 Relevant Legislation

Acceptable use of Social Media must comply with UK law, including, but not limited to:

- [Regulation of Investigatory Powers Act 2000](#)
- General Data Protection Regulations (GDPR) 2018 / [Data Protection Act 2018](#)
- [The Human Rights Act 1998](#)
- [The Equality Act 2010](#)
- [The Defamation Act 2013](#)
- [Copyright, Designs and Patents Act 1988](#)

5.6 Breaches of this policy

All leaders are responsible for ensuring their team read **and** understand this policy.

Complaints relating to the use of social media or the content of posts should be referred to the Headteacher in the first instance. It may also be necessary to inform the Data Protection Officer if complaints involve personal data, including images.

Staff should be aware that breaches of this policy may also breach harassment / IT / equality policies and will be treated as conduct issues.

Suspected breaches of this policy, or complaints received about unacceptable use of social media, will be investigated in line with disciplinary procedures.

Employees are expected to co-operate with any investigation and allow their accounts to be reviewed. They may also be asked to print copies or obtain screenshots of any alleged unacceptable content.

A breach of this policy could lead to disciplinary action and /or dismissal.

This Social Media Policy should be read in conjunction with the IT Security Policy, Online Safety Policy and Bring Your Own Device Policy.

Annex A

Sample platform and account log

Platform	User account name	Master administration role	Approved users (posting)	Date	
				Opened	Closed
E.g. Twitter	History@SSchool	Business Manager	HoD (Humanities)	16/01/21	

Date	Details of Changes	Name	Approval Date	New Version No	Website
23.7.20	<p>New policy cover sheet added</p> <p>Contents page numbering amended</p> <p>Page 3 - The School’s Data Protection Officer (DPO) added to the penultimate paragraph</p> <p>Page 4 - the Headteacher added to the next to last bullet point</p> <p>Page 5 - the Headteacher added to the final sentence</p>	<p>ES</p> <p>JS</p> <p>JS</p> <p>JS</p> <p>JS</p>		Two	
13.5.21	<p>Sentence added to policy cover sheet - This document will be reviewed annually and sooner when significant changes are made to the law</p> <p>Content page updated</p> <p>Section 5.1 – Bullet point 3 information amended and updated</p> <p>Section 5.2 – Largely Re-written and re-formatted</p> <p>Section 5.3 – Complete new section added</p> <p>Section 5.4 – Complete new section added</p> <p>Section 5.5 – Complete new section added</p> <p>Section 5.6 – Complete new Section added</p> <p>Annex 1 – Sample log added to policy</p>	JS		Three	