

Social Media Policy

Policy type	Non-Statutory
Review period	2 Years
Last reviewed on	Spring 2026
Next review due	Spring 2028
Approval level	CEO
Number and Version	025 V1.4
Published on	Staff Area

Version Number	Purpose/Change	Author	Date
V1.1	Scheduled review	Mollie Warne	May-22
V1.2	Update to data protection policy & code of conduct hyperlinks. Removal of Park Campus and Kennington Park website hyperlinks and replaced with Evolve in point 3.	Lizzie Kennedy	May-23
V1.3	Reviewed entirely for March Board Meeting	Angela Barry	March-24
V1.4	Correcting social platform name changes, update to terms of use, addition of Legal and Regulatory Framework, Use of AI and Emerging Technologies, and adding missing social media platforms regularly used.	James Boampong	April-26

CONTENTS

1.	Introduction to the Policy	3
2.	Purpose	3
3.	Scope	3
4.	Use of Images on the Academy's X Account	4
5.	Use of Social Networking Sites in Worktime	4
6.	Use of AI and Emerging Technologies	3
7.	Social Networking as part of Academy Service	5
8.	Terms of Use	5
9.	Guidance/protection for Staff on using Social Networking	5
10.	Guidance/protection for Pupils on using Social Networking	6
11.	Child Protection Guidance	6
12.	Cyber Bullying	6
	Appendix 1: Useful Links	8

1. Introduction to the Policy

- The Parallel Learning Trust is aware and acknowledges that increasing numbers of adults and children are using social networking sites. Some with the widest use are Instagram, Facebook , (X) (formerly known as Twitter), You Tube & Tik Tok.
- The widespread availability and use of social networking application bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our reputation.
- This policy and associated guidance is to protect staff and advise academy/Trust leadership on how to deal with potential inappropriate use of social networking sites.
- For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.
- The policy requirements in this document aims to provide this balance to support innovation whilst providing a framework of good practice.

2. Purpose

The purpose of this policy is to ensure:

- That the Parallel Learning Trust is not exposed to legal risks.
- That the reputation of the Parallel Learning Trust is not adversely affected.
- That our users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the academy/Trust.
- To ensure that our employees do not post anything on social media that they would not be happy wearing as a post-it note on their foreheads...
- To ensure that all staff colleagues are aware that whatever is posted is out there, somewhere forever...
- Safeguarding of pupils, staff and the wider community
- Compliance with UK GDPR, the Data Protection Act 2018 and safeguarding legislation

3. Scope

- This policy covers the use of social networking applications by all academy/Trust stakeholders, including, employees, governance colleagues and pupils. These groups are referred to collectively as 'academy representatives' for brevity.
- The requirements of this policy apply to all uses of social networking applications which are used for any academy/Trust related purpose and regardless of whether the academy representatives are contributing in an official capacity to social networking applications provided by external organisations.
- Social networking applications include, but are not limited to:
 - Blogs, for example Blogger
 - Online discussion forums, such as netmums.com
 - Collaborative spaces, such as Facebook
 - Media sharing services, for example YouTube
 - 'Micro-blogging' applications, for example X
- All academy representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the academy's Equality and Diversity Policy. The Academies Equality and Diversity Policies can be found under each of their Documents and Policies pages:
 - Evolve Academy <https://evolveacademy.org.uk/>
 - Ramsden Hall Academy <https://ramsdenhall.org.uk>
 - Sutton House Academy <https://suttonhouse.org.uk>
 - Victory Park Academy <https://victorypark.org.uk>
 - Wandle Valley Academy <https://wandlevalleyacademy.org.uk>

4. Use of Images on the Academy's X Account

- It is important for all academy representatives using the academy/Trust 'X' to be aware of copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. Any images that are used on the academy/Trust X page need to be copyright free.
- All academy representatives need to be aware of what they are publishing on the academy/Trust X page and hold up to date consent forms from all parents/carers. If you do not hold an up-to-date consent form of an individual pupil do not use their images.

Section 12 of the Trust's [Data Protection Policy](#) states:

"As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

- *Within school on notice boards and in school magazines, brochures, newsletters, etc.*
- *Outside of school by external agencies such as the school photographer, newspapers, campaigns*
- *Online on our school website or social media pages*

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified."

To read our full Data Protection Policy visit <https://plt.org.uk/governance/policies>

5. Use of Social Networking Sites in Worktime

- Use of social networking applications in work time for personal use only is not permitted, unless permission has been given by the Headteacher/CEO.

6. Use of AI and Emerging Technologies

- AI tools must not be used to generate images, videos or content involving pupils without approval
- Deepfake or manipulated content involving members of the Trust is strictly prohibited
- AI-generated content must be reviewed and approved before publication

7. Social Networking as part of Academy Service

- All proposals for using social networking applications as part of an academy/Trust service (whether they are hosted by the academy/Trust or by a third party) must be approved by the Headteacher/CEO first.
- Use of social networking applications which are not related to any academy/Trust services (for example, contributing to a wiki provided by a professional association) does not need to be approved by the Headteacher/CEO. However, academy representatives must still operate in line with the requirements set out within the policy.
- Academy representatives must adhere to the following Terms of Use. The Terms of Use below apply to all uses of social networking applications by all academy representatives. This includes, but is not limited to, public facing applications such as open discussion forums and internally-facing uses such as project blogs regardless of whether they are hosted on academy/Trust network or not.
- Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. Parallel Learning Trust expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

8. Terms of Use

Social Networking applications:

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the academy/Trust into disrepute.
- Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns.
- Must not be used in an abusive or hateful manner.
- Must not be used for actions that would put academy representatives in breach of academy/Trust codes of conduct or policies relating to staff.
- Must not breach the academy/Trust misconduct, equal opportunities or bullying and harassment policies.
- Must not be used to discuss or advise any matters relating to academy/Trust matters, staff, pupils or parents/carers.
- No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with.
- Employees must not present personal views as those of the Trust and should include a disclaimer where appropriate.
- References should not be made to any staff member, pupil, parent/carers, academy or Trust activity/event unless prior permission has been obtained and agreed with the Headteacher/CEO.
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the academy/Trust or detrimentally affects the academy/Trust's reputation then the academy/Trust is entitled to take disciplinary action.

Legal and Regulatory Framework:

- All users must comply with relevant legislation and statutory guidance, including:
- Keeping Children Safe in Education (KCSIE)
- UK GDPR and Data Protection Act 2018

- Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010
- Malicious Communications Act 1988

Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

Section 1.18. of the Trust's [Code of Conduct Policy](#) states:

“The Trust reserves the right to take action against any employee whose actions and/or behaviour, inside or outside work could reasonably be regarded as bringing the Trust into disrepute. This includes the use of social media.”

9. Guidance/Protection for Staff on using Social Networking

- For any/all social media platforms - please adhere to their individual privacy policies which can be found on their websites or via the links in appendix 1.
- No member of staff should interact with any pupil in the academy on social networking sites unless from the academy/Trust Teams, Google Classroom, X account or any other official messaging platforms.
- No member of staff should interact with any ex-pupil in the academy on social networking sites who is under the age of 18.
- This means that no member of the academy/Trust staff should request access to a pupil's area on the social networking site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.
- Where family and friends have pupils in the academy/Trust and there are legitimate family links, please inform the Headteacher/CEO in writing. However, it would not be appropriate to network during the working day on academy/Trust equipment.
- It is illegal for an adult to network, giving their age and status as a child.
- If you have any evidence of pupils or adults using social networking sites in the working day, please contact the named Child Protection/DSL person in the academy.

10. Guidance/Protection for Pupils on using Social Networking

- For any/all social media platforms - please adhere to their individual privacy policies which can be found on their websites or via the links in appendix 1.
- No pupil may access social networking sites during the academy working day unless they have been asked to access a specific social networking site by a member of staff.
- All pupil mobile phones must be handed into the office at the beginning of the academy day, the internet capability must be switched off.
- No pupil should attempt to join a staff member's areas on networking sites. If pupils attempt to do this, the member of staff is to inform the Headteacher. Parents/carers will be informed if this happens.
- No academy computers are to be used to access social networking sites at any time of day unless for direct academy use (posting academy information of the academy Facebook page).
- Any attempts to breach firewalls will result in a ban from using academy ICT equipment other than with close supervision.
- Please report any improper contact or cyber bullying to the class teacher in confidence as soon as it happens.
- We have a zero tolerance to cyber bullying.

11. Child Protection Guidance

- If the Headteacher receives a disclosure that an adult employed by the academy is using a social networking site in an inappropriate manner as detailed above they should:
 - Speak to the CEO/HR as soon as possible.
 - Please refer to relevant section in safeguarding policy.

12. Cyber Bullying

- By adopting the recommended no use of social networking sites on academy premises, other than the academy's X page, Parallel Learning Trust protects themselves from accusations of complicity in any cyber bullying through the provision of access.
- Parents/carers should be clearly aware of the academy's policy of access to social networking sites.
- Where a disclosure of bullying is made, Academies now have the duty to investigate and protect, even where the bullying originates outside the academy.
- This can be a complex area, and these examples might help:
 - A child is receiving taunts on Snapchat and text from an ex-pupil who moved three months ago: This is not an academy responsibility, though the academy might contact the new academy/school to broker a resolution.
 - A child is receiving taunts from peers. It is all at weekends using WhatsApp groups. The pupils are in the academy: The academy has a duty of care to investigate and work with the families, as they attend the academy.
 - A child is receiving taunts from peers. It is all at weekends using TikTok. The pupils are in Y5: This is the tricky one. The academy has a duty of care to investigate and work with the families, as they attend the academy. However, they are also fully within their rights to warn all the parents/carers (including the victim) that they are condoning the use of TikTok outside the terms and conditions of the site and that they are expected to ensure that use of the site stops. At any further referral to the academy, the academy could legitimately say that the victims and perpetrators had failed to follow the academy's recommendation. They could then deal with residual bullying in the academy, but refuse to deal with the social networking issues.
 - Once disclosure is made, investigation will have to involve the families. This should be dealt with under the academy's adopted anti bullying policy.
 - If parents/carers refuse to engage and bullying continues, it can be referred to the police as harassment.
 - This guidance can also apply to text and mobile phone cyber bullying.
 - If a parent/carer is making threats online against a member of academy/Trust staff – this is counted as bullying. The member of staff must inform the Headteacher/CEO immediately and the parent/carer spoken to. Should the situation not be resolved, the police and LA should be informed.

Appendix 1: Useful Links

Instagram

- Help Centre: <https://help.instagram.com>
- Data Policy: https://help.instagram.com/519522125107875/?maybe_redirect_pol=0

YouTube

- Help Centre: <https://support.google.com/youtube/?hl=en#topic=9257498>
- Privacy Policy: <https://policies.google.com/privacy?hl=en>

Facebook

- Help Centre: <https://www.facebook.com/help>
- Data Policy: <https://www.facebook.com/privacy/explanation>

X

- Help Centre: <https://help.x.com/en>
- Privacy Policy: <https://x.com/en/privacy>

TikTok

- Help Centre: https://support.tiktok.com/en/?enter_method=bottom_navigation
- Privacy Policy: <https://www.tiktok.com/legal/privacy-policy-eea?lang=en>
- Privacy Policy (younger users): https://www.tiktok.com/legal/privacy-policy-for-younger-users?enter_method=bottom_navigation

Snapchat

- Snapchat Support: <https://support.snapchat.com/en-GB>
- Privacy Policy: <https://www.snap.com/en-GB/privacy/privacy-policy>

WhatsApp

- Help Centre: <https://faq.whatsapp.com>
- Privacy Policy: <https://www.whatsapp.com/legal/privacy-policy/?lang=en>

Pinterest

- Help Centre: <https://help.pinterest.com/en-gb>
- Privacy Policy: <https://policy.pinterest.com/en-gb/privacy-policy>

Reddit

- Reddit Help: <https://reddit.zendesk.com/hc/en-us>
- Privacy Policy: <https://www.reddit.com/policies/privacy-policy>

LinkedIn

- Help Centre: <https://www.linkedin.com/help/linkedin?lang=en>
- Privacy Policy: <https://www.linkedin.com/legal/privacy-policy>

Tumblr

- Help Centre: <https://help.tumblr.com/hc/en-us>
- Privacy Policy: <https://www.tumblr.com/privacy>

Skype

- Help Centre: <https://support.skype.com/en/skype/all/>
- Privacy Policy: <https://privacy.microsoft.com/en-gb/privacystatement>

Discord

- Help Centre: <https://discord.com/privacy>
- Privacy Policy: <https://support.discord.com/hc/en-us>