REACH SOUTH ACADEMY TRUST

# SOCIAL MEDIA POLICY

# CONTENTS

## 1. Policy statement

1.1 We recognise that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as WhatsApp, Facebook, X, (formerly known as Twitter), Instagram, TikTok, LinkedIn, blogs and wikis.

1.2 However, employees' use of social media can pose risks to our ability to safeguard children and young people, protect our staff, protect confidential information, uphold our reputation and comply with data protection and other legal obligations.

1.3 This could also be the case during non-working hours.

1.4 All staff using social media are also potentially at risk of others misunderstanding the intent behind online communications or blurring of professional boundaries between children and young people and their parents or carers or with other work colleagues. This policy therefore sets out the Trust's expectations regarding the use of social media.

1.5 To minimise these risks, to avoid loss of productivity and to ensure that our IT resources and communications systems/platforms are used only for appropriate business purposes, and that the use of personal devices does not have an adversary impact on our business we expect employees to adhere to this policy.

1.6 This policy is designed to ensure compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. All staff must handle personal data in accordance with these laws when using social media. Any accidental disclosure of personal data on social media must be reported immediately to the Data Protection Officer (DPO) as a potential data breach.

1.7 This policy does not form part of any employee's contract of employment, and it may be amended at any time in consultation with the recognised Trade Unions.

## 2. Diversity, Inclusion and Belonging Statement

2.1 At Reach South Academy Trust, we are committed to creating a vibrant and inclusive environment that celebrates diversity and fosters a sense of belonging for all. This commitment extends to every aspect of our work; from the education we deliver to the staff we employ. We believe in fairness, equity, and promoting social mobility for all.

2.2 We actively promote inclusivity through our People policies and practices. We value and respect every individual, regardless of background, and strive to build a diverse staff and student body that reflects the richness of the communities we serve.

2.3 We dismantle barriers to opportunity by ensuring equal access to resources and development opportunities for all staff members. Our People policies are designed to be fair and unbiased, promoting a level playing field for career progression regardless of social or economic background.

2.4 Serving Our Local Communities: We actively engage with local communities to understand their needs and perspectives. Our recruitment practices prioritise attracting talent from diverse backgrounds within our local area, further strengthening the connection between the Trust and the communities it serves.

2.5 Our People policies are developed and implemented in accordance with the Equality Act 2010. We are committed to eliminating all forms of discrimination on the grounds of age, disability, gender reassignment, marriage/civil partnership, pregnancy/maternity, race, religion or belief, sex, and sexual orientation. This ensures an environment characterised by dignity and respect, free from harassment, bullying, and victimisation.

2.6 These commitments extend to the use of social media. Staff are expected to uphold the Trust's values of dignity, respect, and inclusion in all online activity. Discriminatory, harassing, exclusionary, or offensive content, whether posted during or outside of work, may undermine our inclusive culture and will be treated as a potential breach of this policy and the Trust's Diversity, Inclusion and Belonging Policy.

## 3. Who is covered by the policy?

3.1 This policy covers all employees working at all levels and grades. It also applies to, Trustees, Governors, consultants, contractors, casual and agency staff and volunteers (collectively referred to as staff in this policy). Pupils' use of social media and online platforms is addressed within the Trust's Behaviour Policy and associated policies, including Online Safety and Acceptable Use, which set out expectations for conduct both in and outside of school.

3.2 Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

## 4. Scope and purpose of the policy

4.1 This policy deals with the use of all forms of social media, including WhatsApp, Signal, Snapchat, Facebook, X (formerly known as Twitter), Instagram, TikTok, LinkedIn, all other social networking sites, and all other internet postings, including blogs.

4.2 It applies to the use of social media for both business and personal purposes, whether during working hours or otherwise.

4.3 The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff.

4.4 This policy also applies to the creation, sharing, and storage of any content that includes personal data. Staff must apply the principles of data minimisation and confidentiality when posting online. Social media content may be subject to Subject Access Requests (SARs) under UK GDPR.

4.5 A breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach.

4.6 Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details for work equipment or accounts.

4.7 Staff may be required to remove internet postings which are deemed to constitute a breach of this policy.

4.8 Failure to comply with such a request may in itself result in disciplinary action.

## 5. Personnel responsible for implementing the policy

5.1 The Trust Board has overall responsibility for the effective operation of this policy but has delegated day-to-day responsibility for its operation to the Chief Executive Officer (CEO) and the Director of People.

5.2 Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the CEO and the Director of People.

5.3 All managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

5.4 All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it.

5.5 Any misuse of social media should be reported to the Headteacher (academy-based staff) and People Business Partner or the relevant Director.

5.6 Questions regarding the content or application of this policy should be directed to the same people.

5.7 Managers must ensure compliance with approved communication platforms.

5.8 Staff are responsible for using only approved systems and reporting any misuse or concerns to their line manager or to the ICT team.

## 6. Compliance with related policies and agreements

6.1 Social media should never be used in a way that breaches any of our other policies.

6.2 If an internet post would breach any of our policies in another forum, it will also breach them in an online forum.

6.3 For example, employees are prohibited from using social media to:

- Breach our ICT user policy.
- Breach any obligations they may have relating to confidentiality.
- Breach our Disciplinary Rules.
- Defame or disparage the Trust or its affiliates, trustees, governors, students, parents and carers, staff, business partners, suppliers, vendors or other stakeholders.
- Harass or bully other staff in any way (cyberbullying).
- Unlawfully discriminate against other staff or third parties or breach our Equal Opportunities Policy.
- Breach our Data protection policies (for example, never disclose personal information about a colleague online).
- Breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).
- Employees must comply with UK GDPR principles, including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality.
- Report any suspected data breach involving social media to the DPO immediately.

6.4 Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the Trust and create legal liability for both the author of the reference and the Trust.

6.5 Use of unapproved platforms may result in disciplinary action, specifically where it leads to breaches of confidentiality, inappropriate messaging, or reputational risk.

6.6 The Trust's Dignity at Work Policy outlines expectations for respectful behaviour and procedures for addressing bullying, harassment, and victimisation, including those that may occur via social media.

6.7 Employees who breach any of the above policies will be subject to a formal investigation following the Trust's Disciplinary Policy which may lead to disciplinary action up to and including dismissal.

6.8 This policy supports compliance with relevant legislation and statutory guidance, including but not limited to:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Equality Act 2010
- Keeping Children Safe in Education (KCSIE)
- Human Rights Act 1998
- Education Act 2002 (safeguarding duties)

## 7. Personal use of social media

7.1 We recognise that employees may work long hours and occasionally wish to use social media for personal activities at work or via our computers, networks, and other IT resources and communications systems.

7.2 Occasional personal use of work equipment is permitted strictly during break or lunch times only. Accessing social media outside of these times, during the school day, is prohibited.

7.3 While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the Trust's business are also prohibited.

7.4 Employees who breach any of the above principles will be subject to a formal investigation which may lead to disciplinary action up to and including dismissal.

7.5 This policy applies to personal social media use where an individual's conduct could reasonably be associated with the Trust, impact professional relationships, compromise safeguarding, breach confidentiality, or damage the Trust's reputation. This includes activity outside working hours and on personal devices.

## 8. Monitoring

8.1 The contents of IT resources, equipment and communications systems are all Reach South Academy Trust Property. Therefore, staff should have no expectation of privacy in any messages, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or

communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

8.2 We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your acknowledgement of this policy and your use of such resources and systems.

8.3 This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, logins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

8.4 We may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

8.5 The Trust, wherever possible, will act promptly to contact website hosts and Internet Service Providers to request the removal of content that may be damaging to the Trust including damaging to any member of staff, Trustee/Governor in the course of their employment with Reach South Academy Trust.

8.6 Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the Trust.

8.7 Monitoring of IT and social media use is conducted under the lawful basis of legitimate interest and for safeguarding, security, and compliance purposes. Monitoring will be proportionate and in line with privacy rights. Data collected during monitoring will be retained only as long as necessary for these purposes.

8.8 For further information, please refer to our ICT user policy.

## 9. Business use of social media

9.1 If your duties require you to speak on behalf of the Trust in a social media environment, you must still seek approval for such communication from head office who may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

9.2 Likewise, if you are contacted for comments about the Trust for publication anywhere, including in any social media outlet, direct the inquiry to head office and do not respond without written approval.

9.3 The use of social media for business purposes is subject to the remainder of this policy.

## 9.4 Management of official school social media accounts

9.4.1 To ensure the secure and effective management of the school's official social media presence, staff designated to administer school social media accounts (e.g., Facebook) are required to access these accounts using their personal Facebook profile. This approach reflects current Facebook/Meta platform functionality, as shared or generic login credentials are no longer supported for Page administration.

9.4.2 Upon logging in with their personal Facebook profile, authorised staff will be added as Page Managers or granted appropriate permissions through Meta Business Suite. This system provides secure, role-based access that allows designated employees to post updates, respond to messages, monitor engagement, and manage content on behalf of the school.

9.4.3 Using a personal Facebook profile for access **does not** provide the school with access to the individual's personal account, activity, or private information. Page Managers must actively switch between their personal profile and the school's business account. Personal content remains private and is neither visible to nor accessible by the school.

9.4.4 Staff with Page Manager roles must exercise their responsibilities in accordance with this Social Media Policy, the Trust's safeguarding and data protection requirements, and all other relevant policies. This includes maintaining professional standards, protecting confidential information, and ensuring that any content published on behalf of the school is accurate, appropriate, and aligned with Trust values.

9.4.5 Staff must use Meta Business Suite responsibly and ensure that all actions taken on behalf of the school uphold safeguarding expectations, comply with UK GDPR and the Data Protection Act 2018, and maintain the school's reputation. Any concerns regarding access, account security, inappropriate content, or potential breaches must be reported immediately to the Headteacher, ICT Security Lead, or Data Protection Officer as appropriate.

## 10. Recruitment

10.1 It is prohibited that any recruitment panel member, either themselves or through a third party, conduct searches on applicants on social media or the internet. This is because conducting these searches during the selection process might lead to unconscious bias or a presumption that an applicant's protected characteristics (for example, sexual orientation or religious beliefs) played a part in a recruitment decision.

10.2 This is in line with the Trust's Diversity, Inclusion and Belonging Policy.

10.3 As part of safer recruitment practices under the *Keeping Children Safe in Education* (KCSIE) statutory guidance, the Trust's Recruitment Team will conduct online searches in line with the guidance for appointed candidates.

## 11. Responsible use of social media

**11.1** Responsible and safe use of social media is essential to protect staff, pupils, and the Trust, while ensuring compliance with UK GDPR, the Data Protection Act 2018, and safeguarding obligations under Keeping Children Safe in Education (KCSIE). These guidelines apply both during and outside working hours and address key risks such as safeguarding, confidentiality, reputational harm, and cybersecurity threats.

### 11.2 Risks

11.2.1 Employees' use of social media can pose risks to:

- Safeguarding children and young people

- Protecting staff
- Maintaining confidentiality
- Preserving the Trust's reputation
- Meeting legal obligations. These risks apply both during working hours and off-duty time

### 11.3 Safeguarding Children and Young People

11.3.1 This section sets out clear safeguarding expectations to protect children and young people by maintaining professional boundaries and ensuring that all communication takes place only through safe, approved Trust channels.

- Staff must not communicate with pupils via personal social media accounts, social networking sites, or personal email accounts.
- Any direct contact from pupils via personal social media accounts must not be responded to, should be blocked, and must be reported to the Designated Safeguarding Lead (DSL) in line with safeguarding procedures.
- Staff must never knowingly engage with pupils on social media platforms, including liking, commenting on, sharing content, or private messaging.
- Staff must not interact on social media with any ex-pupil of the Trust who is under the age of 18.
- All communication with pupils must take place only through Trust-approved systems and in accordance with safeguarding, data protection, and professional conduct requirements.

### 11.4 Protecting Our Business Reputation

11.4.1 Staff must not post disparaging or defamatory statements about:

- The Trust
- Students or their parents/carers
- Trustees, governors or staff
- Suppliers and vendors
- Other affiliates and stakeholders

11.4.2 Avoid social media communications that could be misconstrued and damage the Trust's reputation.

11.4.3 Make it clear when posting that you are speaking on your own behalf. Use personal email addresses for personal social media use.

11.4.4 If disclosing your affiliation with the Trust, state that your views do not represent the Trust (e.g., *"The views expressed are my own and do not represent my employer"*).

11.4.5 Ensure your profile and content reflect a professional image consistent with your role.

11.4.6 Avoid posting about sensitive Trust-related topics, such as performance or internal matters.

11.4.7 If unsure about a post, seek advice from the Headteacher, People Business Partner, or Director of People.

11.4.8 Report any content that may harm the Trust's reputation to the appropriate manager immediately.

11.4.9 Staff should exercise caution when commenting publicly on government policy, Department for Education guidance, or education-related political matters where such commentary could reasonably be perceived as representing the Trust or conflict with their professional role.

### 11.5 Respecting Intellectual Property and Confidential Information

11.5.1 Do not jeopardise the Trust's confidential information or intellectual property through social media use.

11.5.2 Avoid infringing the intellectual property of others, which can create liability for you and the Trust.

11.5.3 Do not use Trust logos, trademarks, or proprietary information without prior written permission.

### 11.6 Respecting Colleagues, Students, Parents, Carers, Trustees, and Stakeholders

11.6.1 Do not post offensive content, including discriminatory comments, insults, or obscenity.

11.6.2 Do not share information about colleagues, students, or stakeholders without written permission.

11.6.3 Do not share personal data of pupils, parents, or staff on social media unless explicitly authorised and necessary for business purposes.

### 11.7 Cybersecurity and Data Protection

11.7.1 This section sets out the Trust's expectations for secure and responsible use of digital platforms, aimed at protecting information, systems, and individuals from cybersecurity threats, data breaches, and emerging risks associated with online and AI-generated content.

- Do not use personal cloud storage or unapproved apps for work-related files or communication.
- Enable Multi-Factor Authentication (MFA) on all approved platforms and maintain strong password practices.
- Be alert to phishing attempts and social engineering via social media. Report suspicious activity to ICT Security immediately.
- Do not engage with AI-generated or manipulated media (deepfakes) that could harm the Trust or individuals.

### 11.8 Prohibited Use of Social Media Platforms

11.8.1 The use of WhatsApp, Telegram, Signal, Snapchat, or any platform not security-assessed and approved by the Trust is strictly prohibited for work-related communication. These platforms do not meet the Trust's standards for data security, auditability, or professional conduct. This prohibition applies regardless of whether accessed via Trust-owned or personal devices.

11.8.2 Examples of prohibited use include:

- Creating or participating in groups for work purposes.

- Sharing pupil, staff, or operational information.
- Using these platforms to coordinate work activities, meetings, or shift arrangements.

### 11.9 Approved Communication Tools and Rationale

11.9.1 All work-related communication must be conducted through Trust-approved platforms for the following reasons:

- **Data Security:** Approved platforms comply with UK GDPR and Trust security standards.
- **Auditability:** Enables monitoring and record-keeping for safeguarding and compliance.
- **Safeguarding:** Ensures safe communication channels for staff and pupils.
- **Cybersecurity:** Approved platforms are regularly updated and protected against threats.

11.9.2 Approved platforms include:

- Microsoft Teams
- Trust email systems
- Any other officially sanctioned communication tools

11.9.3 Public-facing social media platforms (e.g. Facebook, X, Instagram, TikTok, LinkedIn) are not approved communication tools for internal or pupil-related communication. Their use for official Trust messaging is covered in Section 9 (Business use of social media) and requires prior authorisation.

## 12. Incident response and escalation

12.1 All social media incidents involving data breaches, safeguarding concerns, or reputational risk must be reported immediately to:

- **Data Protection Officer (DPO)** for data breaches.
- **Designated Safeguarding Lead (DSL)** for safeguarding concerns.
- **ICT Security Lead** for cybersecurity incidents.

12.2 The Trust will investigate incidents promptly and take appropriate action, including notifying the ICO where required.

## 13. Review of policy

13.1 This policy is reviewed as required by the Trust in consultation with the recognised trade unions.

13.2 We will monitor the application and outcomes of this policy to ensure it is working effectively.

## POLICY HISTORY

| Policy Date | Summary of change | Contact | Implementation Date | Review Date |
|---|---|---|---|---|
| May/June | Trade Union consultation | All Recognised Trade Unions | N/A | N/A |
| June 2020 | New policy implemented | HR | June 2020 | September 2021 |
| June 2022 | Update in line with KCSIE 2022 | HR | October 2022 | June 2024 |
| May 2024 | Amended references from HR to People Team. Inclusion of Instagram Platform and reference to KCSIE 2023. | People Team | June 2024 | May 2026 |
| February 2026 | Addition of Diversity, Inclusion and Belonging (DIB) statement, expanded prohibited use of unapproved messaging platforms (including WhatsApp, Telegram, Signal, Snapchat), introduction of cybersecurity measures (MFA, phishing awareness), and inclusion of GDPR and safeguarding compliance updates. | People Team | February 2026 | September 2028 |
| April 2026 | **DRAFT OUT FOR CONSULTATION:** Clarification of process for managing official school social media accounts, including requirement for Page Managers to access Meta Business Suite via personal Facebook profiles | People Team | April 2026 | September 2028 |