Changes made to the attached policy (Feb 2026)

1. The policy has been reviewed by Judicium and significant additions have been suggested.
2. Section 12 has been suggested by Judicium and is worded so that it forms part of Staff contracts.

The NSB Trust

Social Media Policy

To be reviewed annually

Personnel associated with this Policy:

Data Controller	**Barry Jeffery**
Data Protection Officer	**Judicium**

Contents

1. Introduction

This Policy applies to all Trust staff regardless of their employment status. It sets out the Trust's current practices and required standards of conduct, and all staff are required to comply with its contents. Breach of this policy may result in disciplinary action up to and including summary dismissal in accordance with the Trust's Disciplinary Policy and Procedures. This policy may be amended from time to time and staff will be notified of any changes no later than one month from the date those changes are intended to take effect.

Section 12 is contractual.

2. Purpose of the policy

The Trust recognises that the internet provides unique opportunities to participate in interactive discussions and share information across a wide range of social media platforms. These include, but are not limited to, Facebook, X (Twitter), Instagram, LinkedIn, TikTok, WhatsApp, blogs, wikis, and any other current or future online platforms that enable users to create, share, comment on, or exchange content publicly or privately.

As social media use can pose risks to the Trust's confidential information, reputation, safeguarding responsibilities, and legal compliance, all staff are required to comply with this policy regardless of the platform or technology used.

3. Who is covered by this policy?

This policy covers all individuals working at all levels within the Trust, including senior managers, governors, employees, contractors, trainees, part-time and fixed-term staff, casual and agency staff, volunteers, and third parties with access to Trust systems.

4. Scope and purpose of the policy

This policy applies to all forms of social media and to both work and personal use where there is any connection to the Trust or Trust activities. Improper use may give rise to breaches of contracts, Trust policies, or the law, including:

- bullying, harassment, or unlawful discrimination
- defamation
- contempt of court
- breach of data protection laws
- misuse of confidential information
- damage to the reputation of the Trust or stakeholders

Disciplinary action may be taken regardless of whether the breach occurs during working hours or using Trust equipment. Staff may be required to remove content deemed in breach. Investigations may involve access to Trust-owned accounts, systems or devices, where lawful, proportionate, and necessary.

5. Personnel responsible for implementing this policy

The Trust Board has overall responsibility for this policy and delegates day-to-day responsibility to the Executive Headteacher. All staff are responsible for operating within this policy and reporting misuse. Queries should be directed to the Director of IT Services.

6. Compliance with related policies and agreements

Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

a) breach our electronic information and communications systems policies
b) breach our obligations with respect to the rules of relevant regulatory bodies
c) breach any obligations they may have relating to confidentiality
d) breach our disciplinary rules
e) defame or disparage the Trust, schools within the Trust, its staff, its pupils or parents, its affiliates, partners, suppliers, vendors or other stakeholders
f) harass, sexually harass or bully other staff in any way or breach our anti-harassment and our anti-bullying policy
g) unlawfully discriminate against other staff or third parties or breach our equal opportunities policies
h) breach our Data Protection Policy (for example, never disclosing personal information about a colleague online)
i) breach any other laws or ethical standards (for example, never using social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements) *and*
j) breach our obligations for the Keeping Children Safe in Education publication

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 organisation. Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

7. Personal use of social media

Staff may make lawful personal use of social media outside of work, provided it does not impact the Trust. When using social media personally, staff must:

- make clear views are their own, not the Trust's
- avoid identifying themselves as a Trust employee in ways that suggest they speak for the Trust
- not post content that could bring the Trust, schools, pupils, parents, or colleagues into disrepute
- not disclose confidential Trust information
- ensure online conduct does not undermine suitability to work with children

Former pupils must not be contacted via social media within three years of leaving the Trust. Staff must not accept friend requests from current pupils. The Trust may take action where personal use clearly impacts its reputation, working relationships, safeguarding obligations, or role performance.

8. Monitoring

The Trust reserves the right to monitor, access, and review use of its IT resources and social media accounts where lawful, proportionate, and necessary for safeguarding, compliance, security, or misconduct investigations. Staff should have no expectation of privacy on Trust systems. Monitoring of personal accounts will only occur for lawful, serious concerns.

9. Educational and extra-curricular use of social media

Staff speaking on behalf of the Trust must follow protocols set by the Headteacher and may be required to complete training.

10. Recruitment

The Trust may use internet searches to perform pre-employment checks on candidates during recruitment. Where the School does this, it will act in accordance with its data protection and equal opportunities obligations.

11. Responsible use of social media

The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely.

Photographs for use with social media: any photos for social media posts may only be taken using Trust cameras/devices or devices that have been approved in advance by the Trust's Communications Officer. Where any device is used that does not belong to the Trust, all photos must be deleted immediately from the device, once the photos have been uploaded to a device belonging to the Trust.

Staff protocol for use of social media: where any post is going to be made on the Trust's own social media the following steps must be taken:

a) ensure that specific permission from the child's parent/carer has been sought before the information is used on social media (via parent/carer Photo Consent form). A parent/carer may have provided permission for one social media platform but not another. Staff should ensure that the appropriate permission is specific
b) ensure that there is no identifying information relating to a child/children in the post - for example, any certificates in photos are blank/without names or the child's name cannot be seen on the piece of work. The school should seek additional consent to include any names when posting on social media
c) the post must be a positive and relevant post relating to the children, the good work of staff, the Trust, or positive achievements
d) social media can also be used to issue updates or reminders to parents/guardians. Should staff wish for any reminders to be issued on the main school social account, they should contact their Senior Staff line manager by email to ensure that any post can be issued
e) a member of the Admin Team will post the information, but all staff have the responsibility to ensure that the Social Media policy has been adhered to.

Personal information shared/published on social media will be required to be disclosed under a subject access request.

Protecting our business reputation: Staff should have no expectation of privacy or confidentiality in anything they create or share on social media platforms. When staff create or exchange content using social media they are making a public statement. As such, content will not be private and can be retweeted, copied or forwarded to third parties without their consent. Staff should therefore consider the potential sensitivity of disclosing information (such as sickness absence information) on a platform. Once sensitive or confidential information (or offensive or defamatory information) has been disclosed, it cannot be recovered, and this may result in liability for both The Trust and the member of staff personally.

Staff must bear in mind that, even if they are using social media in a personal capacity, other users who are aware of their association with the Trust might reasonably think that you speak on our behalf. Staff should take account of any adverse impact content might have on The Trust's reputation or our staff, pupils or parents, governors, members, trustees, affiliates, partners, suppliers, vendors or other stakeholders.

When creating or exchanging content on a social media platform, staff must at all times comply with their contract of employment with The Trust, as well as disciplinary rules and any policies that may be relevant.

Staff must use social media responsibly, protect confidential information, and avoid posts that could damage the Trust's reputation. Staff must not:

- harass, bully, or discriminate against colleagues or third parties
- breach the Data Protection Policy or confidentiality obligations
- post abusive, obscene, discriminatory, derogatory, defamatory, pornographic, or sexually suggestive content
- post content belonging to a third party without consent
- accept friend requests or follow students on social media
- post complaints or disparagement about the Trust, schools, pupils, parents, governors, staff, or stakeholders
- express personal views in ways that could be interpreted as representing the Trust

In addition, staff must not post disparaging or defamatory statements about:

- The NSB Trust
- current, past or prospective staff as defined in this policy
- current, past or prospective pupils
- current, past or prospective parents, carers or families of pupils mentioned above
- The NSB Trust's governors, trustees, members, directors, suppliers and services providers, and other affiliates and stakeholders

If staff are uncertain or concerned about the appropriateness of any statement or posting, they should refrain from making the communication until they have discussed it with their Line Manager.

If staff see content on social media that disparages or reflects poorly on The NSB Trust, its staff, pupils, parents, governors, members, trustees, directors, service providers or stakeholders, they are required to report this directly to the Headteacher without unreasonable delay. All staff are responsible for protecting the Trust's reputation.

Staff should regularly review the privacy settings on their personal social media accounts and appropriately restrict the people who can read their posts or comments. They should also review the content of their personal social media accounts on a regular basis and delete anything that could reflect negatively on them in a professional capacity or on The Trust.

Respecting Intellectual Property and Confidential Information

Staff should not do anything to jeopardise The Trust's confidential information and intellectual property using social media.

In addition, staff should avoid misappropriating or infringing the intellectual property of other Trusts, organisations, companies and individuals, which can create liability The Trust, as well as the individual author.

Staff must not use NSB Trust (or individual) logos, slogans or other trademarks, or post any of our confidential or proprietary information without express prior written permission from the Executive Headteacher.
To protect staff and The Trust against liability for copyright infringement, where appropriate, reference sources of particular information posted or uploaded and cite them accurately. If staff have any questions about whether a particular post or upload might violate anyone's copyright or trademark, they should ask their respective Headteacher in the first instance before making the communication.

12. Rights to the NSB Trust's social media accounts

This paragraph forms part of your contract of employment with The NSB Trust

Rights to Trust accounts and any associated databases belong to the Trust. Staff must provide login details on request and on termination. Staff may not retain copies of credentials or contact databases.

13. Monitoring and enforcement

The Trust reserves the right to monitor, access, and review the use of Trust IT systems and social media accounts, including Trust-owned devices and accounts, where lawful, proportionate, and necessary for safeguarding, policy compliance, security, or investigation of misconduct.

Staff should have no expectation of privacy when using Trust systems or Trust-owned accounts.

Monitoring of personal accounts will only occur for lawful reasons, such as safeguarding concerns or serious misconduct.

Disciplinary Enforcement

Any breach may result in disciplinary action, up to and including summary dismissal.

Breaches may also constitute a criminal offence and may be referred to external agencies.

Staff may be required to remove content deemed in breach, and failure to do so may itself result in disciplinary action.

Investigations will be conducted fairly and proportionately, and staff must cooperate, including providing access to Trust-owned accounts/devices where lawful.

Escalation: minor breaches may lead to warnings or remedial action; serious breaches may lead to suspension, formal disciplinary proceedings, or referral to external authorities.

Off-duty or personal social media use may be investigated if it impacts Trust reputation, safeguarding, or employment relationships.

The Executive Headteacher shall be responsible for reviewing this policy annually to ensure that it meets legal requirements and reflects best practice. The Trust Board has responsibility for approving any amendments prior to implementation.

The Headteacher of each school within the Trust has the responsibility for ensuring that any person who may be involved with administration or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.

If staff have any questions about this policy or suggestions for additions to be considered upon review, staff may do so by emailing their Headteacher.

14. Password handover and shared account access

All Trust social media accounts are Trust assets. Passwords and access credentials must:

- be held securely in line with Trust IT security requirements
- be accessible to at least two authorised staff
- not be shared informally

Account managers must:

- provide up-to-date login details to the Director of IT Services (or nominee) on request
- hand over access during absences, role changes, or on request
- ensure account recovery details are registered to Trust-owned contact information

Failure to comply may result in disciplinary action.

15. Account creation, ownership and closure

Only authorised staff may create Trust social media accounts with prior approval. Accounts must:

- use Trust-owned email/contact details
- be recorded in a central register
- clearly identify the account as Trust or school
- comply with this policy and platform guidance

Accounts may only be deleted, archived, or transferred by authorised staff.

16. Staff departure and emergency access

All account credentials must be handed over prior to departure. Access must be immediately revoked for departing staff. Scheduled posts or campaigns must be reassigned.

In emergencies (safeguarding or reputational), authorised staff may access accounts regardless of former staff consent. Former staff must not retain passwords, credentials, or databases.

The Headteacher of the school may authorise emergency access to accounts and must ensure proper records are kept.