



Social Media Policy

Author	O Benzie	Source	National Online Safety
Approved By	ELT	Status	Non statutory
Last Review	June 2026	Next Review	June 2028

Details of Policy Updates

Date	Details
June 2024	Reflect change in policy
June 2026	Changed Facebook to Instagram

1. Introduction and purpose

The purpose of this policy is to provide guidance on the appropriate use of social networking sites by school staff by:

- a. advising staff to ensure that children are safeguarded.
- b. advising staff to ensure that the reputation of the school is not adversely affected through use of social networking sites.
- c. ensuring that the school is not subject to legal challenge as a result of school employees using and providing information on social networking sites e.g. data protection, discrimination and other sensitive information.

This policy should be read alongside the following policies and documents:

- Safeguarding and child protection policy
- Code of Conduct
- Data protection policy
- Keeping Children Safe in Education
- Online Safety Policy

2. Social Networking Sites/Applications

Social networking applications include, but are not limited to: Blogs, Online discussion forums, Collaborative spaces, Media sharing services, 'Microblogging' applications. Examples include Twitter, Facebook, MSN, YouTube, Instagram, Tik Tok, Snapchat, Tumblr, Flickr and Vimeo.

3. Staff Conduct

The North Star Code of Conduct states "All employees have personal and legal responsibilities, including; treating others with dignity and respect; acting honestly, using public funds and school equipment appropriately, adhering to health and safety guidelines and practising equal opportunities at all times" and "All trust staff are expected to demonstrate consistently high standards of personal and professional conduct and maintain high personal standards of ethics and behaviour both in and outside school" These principles apply to the

personal and professional use of social networking sites and messaging groups such as WhatsApp.

The way in which school staff present and conduct themselves on social networking sites can have an impact on the public perception of the school and influence the way in which those staff members are perceived by pupils and parents of the school. In their use of social networking sites, staff should be aware that their online behaviour could affect their professional standing, dignity and perception of their integrity.

It is recommended that school staff take adequate precautions when using social networking sites/applications, both in vetting material that could be connected to them (through their own profile and information added about them) and through the use of appropriate security settings.

School employees must not be “friends” with or follow pupils on social networking sites as this could be viewed as a safeguarding issue. Trust employees must act in the best interests of the Trust and comply with your obligations of confidentiality at all times and not disclose personal data or information about any individual including staff, young people, children or other members of the school community. Staff must not post images or names of students on their personal social media accounts, unless it is sharing a post from LinkedIn.

Where email and learning platforms are used to communicate with pupils, e.g. about homework, this must only be done using a school email address.

Where pupils behave inappropriately towards staff online this should be logged on CPOMS and the safeguarding team will identify the need for any further action.

Trust employees must not access social networking websites for personal use (i.e. non-job-related use) on work equipment.

The Trust respects an employee's private life. However, it must also ensure that confidentiality and its reputation are protected and staff are encouraged to exercise discretion and use social media responsibly at all times. The Trust

must also ensure relevant protection for its operations, confidential information and reputation. If using social networking websites at work or in your private life, including closed groups (e.g. but not limited to What's App or similar) you must not;

- Identify yourselves as working for the Trust, in a way which has, or may have, the effect of bringing the trust into disrepute.
- Identify other school employees, children or young people or other members of the trust community without their consent.
- Avoid making any social media communications that could damage the Trust's business, operations or reputation, even indirectly.
- Defame or disparage the trust
- Harass, bully or unlawfully discriminate against its employees, children, young people, or any other members of the trust community or third parties.
- Conduct themselves in a way that is detrimental to the Trust.
- Disclose personal data or information about the Trust, school, employees, children, or young people, or any other member of the trust community that could breach the Data Protection legislation, for example, posting photographs or images of children or young people.
- Allow pupils to access their personal social networking accounts. Where they are contacted by a pupil they should bring it to the Headteacher's attention.
- Make false or misleading statements.
- Impersonate colleagues or third parties;
- Express opinions on the Trust's behalf using social media, unless expressly authorised to do so by your Head Teacher; you may be required to undergo training in order to obtain such authorisation.
- Post comments about sensitive business-related topics, such as draft proposals or information belonging to any organisation (or person) with which the Trust works in partnership.
- Do anything to jeopardise our confidential information and intellectual property.
- Include our logos or other trademarks connected to the Trust's work in any social media posting or in your profile on any social media.

Communications for these purposes includes the use of words and images.

Employees who wish to set up personal web-forums, weblogs or 'blogs' must do so outside of work, not using school equipment and adhere to the points detailed above.

Note- Explicit Images or Sexting. Sending naked images can be a crime. Sharing explicit images without the person's consent is illegal. Should it be brought to the trust's attention that such images have been shared or should such images become public it could lead to disciplinary action up to and including dismissal for all parties employed at the Trust. Be aware that even images which self-destruct after a few seconds can be saved by the recipient. Problems normally arise after a relationship ends but could also arise if the sender or recipient's phone is accessed by a third party e.g. a child.

4. The School LinkedIn and Instagram Account

The school LinkedIn and Instagram account allows us to share information (including weblinks, images or video clips as appropriate) about our school. It can be used effectively to engage parents, to share and celebrate our successes and to showcase our practice.

There is one Trust LinkedIn account, and one Instagram account and staff should not set up additional subject accounts.

Guidance for posts on the school account:

- We must have parental consent for any pupil whose photo appears on social media. See Arbor for the parental consent list;
- The first names of students can be used alongside the photo but surnames must not be used;
- All posts must be respectful in nature and promote the positive aspects of school life.