Social Media Policy

Version 6.0

Important: This document can only be considered valid when viewed on the Trust's website. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.	
Name of Author	Trust ICT Manager
Name of Responsible Committee/Individual	Trust Board
Date Policy Agreed	April 2021 (Version 1) May 2022 (Version 2) December 2022 (Version 3) July 2023 (Version 4) July 2024 (Version 5) July 2025 (Version 6)
Review Date	July 2026
Target Audience	All Stakeholders
Related Documents	Acceptable Use Agreement - Staff Acceptable Use Agreement – Parent/Student Code of Conduct Digital Safety Policy Data Protection Policy

CONTENTS

1. Rationale

Brighter Futures Learning Partnership Trust recognises and embraces the numerous benefits and opportunities that social media offers. While staff and students are encouraged to engage, collaborate, and innovate through social media, they must also be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation.

2. Purpose

The purpose of this policy is to encourage good practice, to protect the Trust, school, staff, students, and to promote the effective use of social media as part of the school/trust activities.

This policy covers personal and professional use of social media and aims to encourage its safe use by the school, its staff, parents/carers, and students.

The policy applies regardless of whether the social media is accessed using the Trust/school IT facilities and equipment, or personal equipment

Personal communications made via social media accounts that could negatively affect professional standards or the reputation of the Trust or school fall within the scope of this policy. This includes posting, sharing, reacting to, or engaging with inappropriate content, including posts made by others that may be linked to the Trust or school

This policy covers all individuals working at all levels and grades, including full-time and part-time employees, fixed-term employees and agency workers. It also covers parents/carers and students.

3. Roles, responsibilities

Trust CEO, Trust Board and Trustees

Responsible for ensuring policies are maintained and checked each year and that each school is implementing the policies.

School Governors, the Headteacher/Principal

Responsible for the implementation of the Social Media Policy and for monitoring the effectiveness.

Staff

Staff must:

- Be aware of their online reputation and recognise that their online activity can be seen by others including parents, students, and colleagues on social media
- Ensure that any use of social media is carried out in line with this policy and other relevant policies, i.e. those of the employer
- Be aware that any inappropriate use of social media in school/college may result in disciplinary action

- Be responsible for their words and actions in an online environment. They are therefore advised to consider whether any comment, photograph, or video that they are about to post online is something that they want students, colleagues, other employees of the Trust, or even future employers, to read.
- Be responsible for the privacy settings of their own accounts and awareness of who can access their information and posts.

Line Managers and Senior Leaders

Line managers and senior leaders are responsible for:

- Addressing any concerns and/or questions employees may have on the use of social media
- Raising concerns with the headteacher/principal where social media has been misused
- Operating within the boundaries of this policy and ensuring that all staff understand the standards of behaviour expected of them.

Parents/Carers

Parents/Carers are responsible for:

- The responsible use of social media in relation to their children in the school
- Using the correct channels of communication (i.e. not social media) for issues or concerns arising from the education of their children
- Reporting any concerns or issues to the school as quickly as possible
- The privacy settings of their own accounts and awareness of who can access their information and posts.

Students

Students are responsible for:

- Reporting any concerns or issues as soon as possible
- Trustworthy use of social media
- Not bringing the school or Trust into disrepute
- The privacy settings of their own accounts and awareness of who can access their information and posts.

4. Definition of social media

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. It allows people to share information, ideas, and views. Examples of social media include blogs, Facebook, LinkedIn, X, Instagram, TikTok, Snapchat, WhatsApp, Flickr and YouTube. This however is not an exhaustive list.

5. Acceptable use

Be aware that content uploaded to social media is not private. Even if you restrict it to ‘friends’, there is still capacity for it to be re-posted or distributed beyond the intended recipients.

Therefore, those who use social media must conduct themselves with professionalism and respect.

Staff

Staff must not upload, repost, comment, or interact, nor should they knowingly allow others to upload any content on to social media sites that:

- Is confidential to the school/Trust or its staff
- Amounts to bullying
- Amounts to unlawful discrimination, harassment, or victimisation
- Brings the school/Trust into disrepute
- Contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images or video clips
- Undermines the reputation of the school and/or individuals
- Is defamatory or knowingly false
- Breaches copyright
- Is in any other way unlawful
- Remember that anything you post online is not completely private. Below are some common-sense guidelines and recommendations that staff are advised to follow to ensure responsible and safe use of social media.

Staff must:

- Not interact with, including liking, commenting, or sharing content online that may damage the reputation of the Trust, school, or individuals
- Not engage in gossip or speculation about Trust/school related incidents on social media, including private groups or messenger platforms as these can be shared by a third party.
- Not use social media to express frustration about work-related matters. Use the correct internal procedures to raise concerns either through line management or the Headteacher/Principal. If it is a serious concern this can be escalated to the Trust.
- Not post anonymously or under an alias to make derogatory, misleading, or malicious statements about the Trust, its staff, students or operations
- Report immediately to the Headteacher/Principal/CEO and not engage in any content posted by others (staff, students, or third parties) that concerns the Trust or a school and know that failure to do so may be considered a breach of duty.
- Not add students (ex-students under the age of 18) as friends or contacts in your social media accounts.
- Always maintain professional boundaries.
- Not use personal accounts to communicate with any student or parent/carer.
- Not engage in discussion with students or parents online unless through official school accounts.
- Decline friend requests from parents. Think about the potential risks to professional boundaries of adding parents to your private social media accounts (if a parent requests or contacts you through social media you should alert your line manager).
- Consider using an alternative name on social media sites to make it harder for students to find you. For example, some members use their partner's surname online but their own surname in school.
- Remember humour is relative. Consider whether your images and/or text may be deemed as inappropriate. Likewise, a few 'light-hearted' comments and/or images

about colleagues or students may not be perceived as such by either subject(s) of the humour or the employer. The guiding rule is: if in doubt, don't post it.

- If you are tagged in something in that you consider inappropriate, use the remove tag feature to un-tag yourself where possible (review the help centre of the Social Media platform in question for support).
- Be cautious of accepting 'friend requests' from people you do not really know. Simply being a 'friend' of your own friend does not mean that they should automatically be given access to your information.
- Review your profile information and settings on all social media platforms to ensure it is appropriate as it may be accessed by others such as colleagues, students, parents, and potential employers.
- Check your privacy and security settings regularly and keep your date of birth and home address to yourself. Identity theft is a growing crime, and this kind of information could be used to gain access to your bank or credit card account.
- Never post any information which can be used to identify a student. This can only be done through official social media accounts with express permission from the student/parent/guardian.
- Never upload, repost, comment, or interact on content, whether public or private social media platforms, that could bring the Trust into disrepute, including posts by others.
- Respect student privacy and confidentiality always.
- Use strong passwords for social media accounts and change them regularly. Protect mobile phones smart phones/tablet computers with at least a PIN, especially when in school to protect access to its content and potential misuse.
- Do not use social media to 'whistle blow' – raise concerns through the proper channels which would entitle you to legal protection (Public Interest Disclosure Act 1998).

The use of social media accounts during lesson time is not permitted.

Any social media account or online resource related to the School or Trust can only be created with approval from the Trust IT Manager and the CEO. Social media is a valuable tool for communication between the Trust, schools, students, parents, and carers, but it must be used appropriately and safely. Staff members must obtain written permission from the Headteacher/Principal before setting up any social media resource. The Headteacher/Principal is ultimately responsible for all posts and may delegate this responsibility to someone who has the authority and training to vet postings. Anything which is found to bring the school or Trust into disrepute must be removed immediately.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

The following procedures must always be observed:

- When using digital images, staff must inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They must recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff can take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution, and publication of those images. Those images must only be taken using school equipment; the personal equipment of staff must not be used for such purposes. They must also only be stored on the Trust and school ICT systems and not on any personal device.
- Care must be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals, Trust or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on websites, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs of students are published on the school/Trust social media platforms, including school/Trust websites (this is covered as part of the agreement signed by parents or carers).
- Be aware that downloading, copying, or printing images from the internet may also breach copyright laws.

Access to Inappropriate content

Some internet activity e.g., accessing child abuse images or distributing racist material is illegal and is obviously banned from the schools/Trust and all other ICT systems. Other activities e.g., cyber-bullying, use of electronic communications to radicalise children or others, is banned, and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. For safeguarding purposes, some access may be required to this content in the course of an investigation, but this is closely managed and monitored by the Trust ICT Manager.

Parents/Guardians

Parents/Guardians must:

- Not post photos, videos or comments that include other children at the school.
- Not use social media on their own devices while on school premises.
- Not access social media while helping at school or on school visits.
- Raise queries, concerns, and complaints directly with the school rather than posting them on social media – whether on their own pages, in closed groups (e.g., groups set up for school parents to communicate with each other) or on the school's pages.
- Not post anything malicious about the school or any member of the school community

Students

Students must:

- Not join any social networking sites if they are below the permitted age (13 for most sites including Facebook and Instagram).
- Tell their parents if they are using the sites, and when they are online.
- Be aware how to report abuse and inappropriate content.
- Not access social media on school devices, or on their own devices while they are at school unless with express permission from the teacher as part of their lesson.
- Not make inappropriate comments (including in private messages) about the school, teachers, or other children
- Use a mobile phone or other digital device in a lesson without express permission from the teacher.

6. Safeguarding

The use of social networking sites introduces a range of potential safeguarding risks to children and young people.
Potential risks can include, but are not limited to:

- Online bullying
- Grooming, exploitation, or stalking
- Exposure to inappropriate material or hateful language
- Extremism and radicalisation
- Encouraging violent behaviour, self-harm or risk taking.

In order to mitigate these risks, there are steps you can take to promote safety online:

- You should not use any information in an attempt to locate or meet a child.
- Ensure that any messages, photos, or information comply with existing safeguarding policies as well as this social media policy.

7. Reporting safeguarding concerns

Any content or online activity which raises a safeguarding concern must be reported to the designated safeguarding lead in the relevant school as soon as possible.

Any online concerns must be reported as soon as identified as urgent steps may need to be taken to support the child.

For staff safeguarding, you must report any harassment or abuse you receive online while using your work accounts.

8. Reporting, responding and recording cyberbullying incidents

Staff and students must never engage with cyberbullying incidents. If you discover a website containing inaccurate, inappropriate, or inflammatory written material relating to you, or images of you which have been taken and/or which are being used without your permission, you should immediately report this to a senior manager (as a member of staff) or the designated safeguarding lead if you are a student.

Staff must keep any records of the abuse such as text, emails, voicemail, website, or social media. If appropriate, screen prints of messages or web pages could be taken and the time, date and address of site should be recorded.

9. Breaches of this policy

It is hoped that all members of our Trust and school communities will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse and must be reported immediately to the Headteacher/Principal.

- The Headteacher/Principal must be informed immediately.
- The Headteacher/Principal and any other relevant members of the school SLT must inform the relevant authorities immediately of any concerns/ infringements.
- The steps taken must all be reported to the school's Local Governing Board.

Any suspected breach of this policy (or if complaints are received about unacceptable use of social networking that has potentially breached this policy) will be investigated in accordance with the school/Trust's bullying, disciplinary and safeguarding procedures. Members of staff, students and parents/guardians will be expected to co-operate with the school's investigation which may involve:

- Cooperating fully with any investigation, which may include the sharing of evidence where legally appropriate. The Trust will not request personal passwords but may request voluntary access to content relevant to the investigation.
- Printing a copy or obtaining a screenshot of the alleged unacceptable content
- Determining that the responsibility or source of the content.

The seriousness of the breach will be considered including the nature of the content, how long the content remained visible on the social media site, the potential for recirculation by others and the impact on the school/Trust or the individuals concerned.

Staff engagement with inappropriate content posted by others (e.g., liking, commenting, or sharing) will be treated as participation. Such engagement may be investigated under the Trust's Disciplinary policy. Disciplinary responses may apply even if the original content was not authored by the staff member.

Staff must ensure their online conduct upholds the reputation of the School/Trust and is line with professional expectations. Staff must be aware that actions online can be in breach of the

harassment/IT/equality policies and any online breaches of these policies may also be treated as conduct issues in accordance with the disciplinary procedure. If the outcome of an investigation leads to disciplinary action, the consequences will be dealt with in accordance with the appropriate procedures. Serious breaches could result in the dismissal of the employee.

Students must be aware that any breach will be investigated as laid out in this policy and consequences will be put in place in line with the school's behaviour policy.

Where conduct is considered to be unlawful, the school will report the matter to the police and other external agencies.

10. Investigating Inappropriate Use of Social Media

Following a report of inappropriate use of social media there will be an investigation. For students this may be carried out by the safeguarding team or another appropriate member of staff. For staff, this will be carried out by a senior leader designated by the headteacher/principal.

If during the investigation it is found that a student submitted the material to the website, that student will be disciplined in line with the school's behaviour policy. If it is found that a member of staff is responsible for the material, then procedures in the Disciplinary Policy will be used.

The investigator, where appropriate, will approach the website hosts to ask that the material is either amended or removed as a matter of urgency, i.e. within 24 hours. If the website requires the individual who is complaining to do so personally, the school and Trust will give their full support and assistance.

If the material concerns a member of staff and is threatening and/or intimidating, senior management will, with the member of staff's consent, report the matter to the police. The member of staff will be offered full support and appropriate stress counselling.

Any staff found to be interacting with **any** inappropriate content created by a colleague, will also be subject to appropriate disciplinary proceedings.

11. Monitoring and review

The School and Trust reserve the right to monitor and record all traffic and messages sent using the ICT systems and infrastructure.

This policy will be reviewed on a yearly basis, and in accordance with the following, on an as-and-when-required basis:

- legislative changes
- good practice guidance
- case law
- significant incidents reported.

12. Legislation

Acceptable use of social networking must comply with UK law. In applying this policy, the school/trust will adhere to its rights, responsibilities, and duties in accordance with the following:

- Regulation of Investigatory Powers Act 2000
- General Data Protection Regulations (GDPR) 2018
- The Human Rights Act 1998
- The Equality Act 2010
- The Defamation Act 2013