

Connect Academy Trust

Social Media Policy

**Approved by the Executive Leadership Team of
Connect Academy Trust, September 2026**

Version	Date	Detail
1	03/2021	New policy
2	17/03/2022	No change
3	29/05/2022	Amended policy combined with Coast policy
4	09/2023	Social media of Potential employees of the Trust will come under scrutiny prior to employment.
5	08/07/2024	Reviewed and checked for 2024-2025
6	09/2025	Reviewed and checked for 2025 - 2026
7	19/06/2026	Updated to reflect current social media and AI matters

For Next Review and Approval by the Executive Leadership Team of Connect Academy Trust, September 2027

Contents

1. Key Principles
2. Aims
3. Code of Conduct
4. Potential and Actual Breaches of the Code of Conduct
5. Organisational control
6. Social Media - Protecting Professional Identity
7. Managing your personal Social Media
8. Managing school social media accounts

Social Media Policy

1. Key Principles

All individuals of Connect Academy Trust including Staff, Pupils, Parents, Governors, Volunteers, Directors, Members and external services providers and friends should ensure they conduct themselves, at all times, in such a way that serves to protect the reputation of the Trust, and treat colleagues, pupils and others associated with the Trust with professionalism and respect. This also relates to potential staff where checks will be carried out on social media, prior to employment. Online searches may be carried out on shortlisted candidates as part of the recruitment process in accordance with Keeping Children Safe in Education. The purpose of these searches is to identify any information relevant to a candidate's suitability to work with children.

It is highly important to protect all individuals and schools from being the subject of inappropriate statements and comments placed on social media/networking/messaging sites or similar. This could include statements referring to confidential issues, making false or vexatious allegations, derogatory, insulting or offensive remarks and threats or intimidating comments, as well as negative comments about the school, Trust or anyone associated with the Trust. The posting of such comments will be viewed as a potential breach of policy and appropriate action taken. Where such actions are committed by employees of the Trust it may be viewed as misconduct or gross misconduct and steps may be taken in accordance with the agreed Trust Disciplinary Policy.

Safeguarding children is a key responsibility of all members of staff and it is essential that all individuals consider this and act responsibly when using social media sites or similar. Anyone working in the Trust either as a paid employee or volunteer must not communicate, 'friend' or similar with Connect school children through personal social media accounts, messaging applications, gaming platforms or other personal online communication channels. Staff must not establish personal online relationships with current pupils and should exercise professional judgement regarding former pupils, taking account of safeguarding guidance and the nature of their previous relationship. As it could be difficult to know which school(s) has been attended and to avoid any allegations or similar, the Trust advise that it is usually not appropriate to 'friend' (or similar) any child who is not related. If in any doubt and to avoid putting yourself at risk, check with your headteacher first.

Any social media activity which raises concerns regarding the safety or welfare of a child, or which may indicate that an adult is unsuitable to work with children, will be referred to the Designated Safeguarding Lead and managed in accordance with the

Child Protection and Safeguarding Policy, Allegations Against Staff Procedures and Keeping Children Safe in Education.

It should also be noted that other than in exceptional circumstances and where the prior approval of the headteacher has been given, personal social media or similar should only be accessed during breaks from work and not while working with children.

2. Aims

- To set out the key principles and code of conduct expected of all individuals in the Trust including, Staff, Pupils, Parents, Governors, Directors, Members, Volunteers, external service providers and friends within the Trust with respect to social media.
- To support the Board of Directors overriding commitment to safeguard and protect children, staff and other individuals at the Trust.

3. Code of Conduct

The following are considered unacceptable within Connect Academy Trust:

- The use of the Trust's name, logo, or any other published Trust material for anything other than promotion of the Trust and its schools, without prior written or verbal permission from the CEO.
- The posting of any communication or images which links the Trust to any form of illegal activity or any other action which may damage its reputation. This includes defamatory comments.
- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the Trust.
- The unauthorised posting of any images of employees, children, Governors, Directors, Members, Volunteers or anyone directly connected with the Trust whilst engaged in Trust activities.
- Making derogatory, defamatory, rude, threatening or inappropriate comments about the Trust, or anyone at or connected with the Trust.

In addition to the above requirements, individuals are advised to use social media carefully, responsibly and to ensure that neither their personal or professional reputation, nor the Trust's reputation is compromised in any way by inappropriate or unacceptable postings.

Individuals should also be aware of risks associated with online identity fraud and be cautious when giving out personal information about themselves which may compromise their personal safety and security.

Staff should remain vigilant to signs of radicalisation, extremism or other safeguarding concerns and report concerns through established safeguarding procedures. It is each person's responsibility to report any concerns or suspicious activity immediately to the Computing Lead or Safeguarding Team.

4. Potential and Actual Breaches of the Code of Conduct

In instances where there has been a breach of the terms of this policy by an employee of the Trust, the following will apply:

Any breaches of this policy by an employee of the Trust will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure. Depending on the circumstances a breach of this policy may be viewed as misconduct which could result in disciplinary action being taken or gross misconduct which may result in summary dismissal.

Any breach of this policy by an individual linked to the Trust, who is not an employee of the Trust, the Board of Directors will take appropriate action in order to protect the Trust's reputation and that of the Children, Staff, Parents, Governors, Directors, Members and anyone else directly linked to the Trust.

5. Organisational control

Roles & Responsibilities

- SLT
 - Facilitating training and guidance on Social Media use.
 - Developing and implementing the Social Media policy
 - Taking a lead role in investigating any reported incidents.
 - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- Staff
 - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
 - Attending appropriate training
 - Regularly monitoring, updating and managing content they have posted via school accounts
 - Ensure they sign the Acceptable Use Agreement

Monitoring

School accounts must be monitored regularly and frequently (preferably 5 days a week during term time and occasionally during school holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention are essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media, staff must not provide statements to the media on behalf of the Trust or Academy unless authorised to do so by the CEO or Headteacher.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies and may take action according to the disciplinary policy.
- The standards within this policy apply equally to content created or shared using artificial intelligence (AI) tools. Staff remain responsible for ensuring that any AI-generated content is accurate, professional, lawful and does not breach confidentiality or safeguarding requirements.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.

- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.
- Social media should not be used as a substitute for the Academy's complaints procedure. Concerns should be raised through the appropriate channels to enable them to be addressed effectively.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the data protection policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload pupil pictures online other than via school owned social media accounts and only with permission from parents/carers
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Pupils should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- Staff
 - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
 - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
 - Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- Pupil/Pupils
 - Staff are not permitted to follow or engage with current or prior pupils/pupils of the school on any personal social media network account.
 - The school's education programme should enable the pupils/pupils to be safe and responsible users of social media.
 - Pupils/pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy
- Parents/Carers
 - If parents/carers have access to a school forum where posting or commenting is enabled, parents/carers will be informed about acceptable use.
 - The school has an active parent/carers education programme which supports the safe and positive use of social media. This includes information on the website.
 - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carers to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.
 - Parents/carers should not publish photographs or videos taken at school events on social media if they include children other than their own, unless permission has been obtained from the parents/carers of those children.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

6. Social Media - Protecting Professional Identity

The Academy, schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. The Academy, schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render Connect Academy liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and Connect Academy through limiting access to personal information:

- Training to include: acceptable use, social media risks, checking of settings, data protection and reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Connect Academy Trust staff should ensure that:

- They do not engage in online discussion on personal matters relating to members of the Connect Academy community
- Personal opinions should not be attributed to the Connect Academy Trust or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Connect Academy Trust use of social media for professional purposes will be checked regularly by the senior staff and members of the IT and media teams to ensure compliance with the Social Media, Data Protection and Digital Image Policies.

With official school / academy trust social media accounts, there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under academy disciplinary procedures
- A clear understanding of this policy by all users of the account

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school / academy or impacts on the school/ academy, it must be made clear that the member of staff is not communicating on behalf of the school / academy with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

7. Managing your personal use of Social Media

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Do not use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep a constant eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; scale, audience and permanency of what you post
- If you want to criticise, do it politely and in no way which will jeopardise your professional role
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

8. Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other people's materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process

- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances