GREENWOOD ACADEMIES TRUST

Social Media User Policy

Version 1.0 Approval Status:

Document Owner:	Darren Yarnell
Classification:	External
Review Date:	9 November 2020
Review Cycle:	2 years

Contents

1. Policy Statement

The use of online social media sites (e.g. Facebook, Twitter, LinkedIn etc.) has become a significant part of life for many people. It is also a key part of businesses' communications strategies, to promote and communicate information about the organisation to the world at large.

The Greenwood Academies Trust (GAT) is no exception and embraces social media as we recognise its value and the positive impact it can make.

The Trust has several social media accounts to reach different audiences and currently uses Facebook, Twitter, and LinkedIn. The Trust is also setting up a YouTube account.

Primarily, this policy is intended to support staff to be able to use social media in a safe and positive manner within a professional environment.

We want to ensure that the right teams engage appropriately with the right audience, with support from the Marketing and Communications team.

A Social Media Policy outlines the procedures which must be followed when using it at work. It explains to staff how the use of social media accounts is to be regulated and the consequences of breaching this policy.

When using social media platforms, it is everyone's responsibility to ensure that the procedures described in this document are followed.

This Social Media Policy should be read alongside Social Media User guides and other relevant Trust policies, including the ICT Acceptable Use Policy, E-Safety Policy, E-Safety Procedure, Media Protocol, Data Protection Policy, Whistleblowing Policy and the Staff Code of Conduct.

2. Policy Aims

The aims of the Trust's Social Media Policy are:

- To promote the Trust in a positive manner.
- To ensure staff have clear guidelines and understand the importance of using social media responsibly when using personal accounts.
- To share good practice.
- To utilise each post/comment as an opportunity to highlight we are listening, engaging and responding.

We want to promote a positive framework for staff when using social media both on behalf of the Trust when communicating with parents, pupils and other organisations and also to promote good practice for personal use.

We are aware that social media sites can also become a negative forum for complaining, gossiping or 'flame' messages.

3. Setting up a New Account

All GAT related social media accounts must be set up centrally by the Marketing and Communications team, whose contact details can be found at the end of this document.

If any GAT employee wishes to set up a new social media account, they must e-mail the Marketing & Communications team with the request who will then liaise with IT and their Principal/Director to set the account up securely.

If the social media platform is not currently supported by the Trust, the risks associated with the platform will be reviewed and a decision will be made on whether it is something the Trust can adopt.

Staff must not set up any Trust related social media accounts themselves unless they have permission to do so by the Marketing and Communications team.

4. Deleting an Account

Any account that is no longer actively used or necessary can be deleted by the Marketing and Communications team, at the request of the Academy's Principal or Director. It is not permitted for anyone else to delete a Trust related social media account, unless they have permission from the Marketing and Communications team.

5. Social Media Account Branding

All Trust related social media accounts must be in line with the Trust's branding. That is to say that profile pictures should be the Academy's or Trust's logo and any banner images should be of a high quality.

If the social media account is not a generic Academy account (for example, the Skegness Academy Library Twitter, GAT Safeguarding etc.) the Marketing and Communications team will advise on branding for the account.

Where colour options are available, the GAT brand colours should be selected (see the Trust Branding Guidelines).

6. Users

In order to showcase the great work that takes place across the Trust, each Academy and Director should specifically authorise a relatively small number of staff members as their authorised social media users.

The Academy/Director must inform the Marketing and Communications team/the Academy Principal of any new user they would like to add to their authorised user list.

All new users will have to familiarise themselves with this policy and sign the final page before they can receive an e-mail with the necessary login details, as well as regular social media plans from the Marketing and Communications team.

Only authorised users can access the Trust's social media accounts. Authorised users must not share their login details for any social media account with any other person.

The Marketing and Communications team must be informed of any authorised user leaving the employment of the Trust immediately so that Trust related social media accounts can be protected and the login details reset.

7. Protocol for Corporate/Trust Use

7.1. How staff <u>should</u> use Social Media

- Only authorised users can have access to the Trust's social media accounts.
- Where it is wished for photographs to be taken or film recordings to be made of staff and/or pupils, as individuals, as small groups or organised groups, the individuals concerned must give their consent and be informed of the purposes for which the information is to be used.

Written permission from parents/carers should be obtained before photographs and videos of pupils are taken. Where a pupil reaches the age of 13, written consent will also be sought from them as well as the parent/carer. Pupils aged 13 and above can also give verbal consent on the day but this needs to be recorded. (See E-Safety Procedure and General Data Protection Policy (GDPR)).

- Should a new social media account be set up for an Academy/Director, consent for that particular account will be needed so revised photo permission forms will need to be provided for parents/carers and relevant pupils. (See the GDPR Policy).
- Staff should only take pictures and videos of pupils with password protected equipment, provided by the Trust/Academy. (See E-Safety Procedure and GDPR Policy).
- Authorised users should create frequent and engaging content, including news and updates to keep the accounts active.

7.2. How staff <u>should not</u> use Social Media

- Staff should never share any work-related log-in details or passwords with other people within or outside of the Trust. If staff share the login details with another person, this may be treated as misconduct. (See ICT Acceptable User Policy and the Staff Disciplinary Policy).
- No additional social media accounts associated with the Trust should be created unless advised or approved by the Marketing and Communications team.
- Staff must not post indecent or offensive remarks on or through the GAT social media channels. (See Staff Code of Conduct).
- Staff must not disclose any confidential information on any social media channels about the Trust or its Academies that is not in the public arena. (See E-Safety Procedure).
- Staff must not disclose any personal data or information about, colleagues, pupils, parents, Academy Advisory Council (AAC) members, Trustees or any individuals connected with the Trust. (See E-Safety Procedure).
- Staff must ensure images and videos are not substantially edited, altered or adapted from their original intention or purpose. The use of full name (both first and surname) should not be used without good reason. (See E-Safety Procedure).

All of the above also applies equally to personal use and business use of social media platforms.

8. Protocol for Personal Use

Whilst the Greenwood Academies Trust has no wish to interfere in the private activities of its employees, there could be occasions where such activities could affect the Trust or its Academies. The Trust is mindful of the provisions in the Human Rights Act 1988 which gives a "right to respect for private and family life, home and correspondence", however, there is also a need to protect the reputation of the Trust.

- Staff should always use the highest privacy settings available.
- Staff must be personally responsible for what they communicate on personal social media and that what they publish might be available to be read by the masses, including the employer, in the future as well as the present.

- Staff should be aware that once a comment/image has been shared on social media, they lose control of the comment/image.
- Staff should understand the importance of observing the appropriate protocols for responding to inappropriate contact via social media channels e.g. for a work matter raised on personal social media, staff should reply from their professional email address.
- Staff must ensure that the public view of their personal social media profiles and their public content is consistent with the professional image they present to students, colleagues and their employer.
- Staff should keep their personal contact details private and must not use their own mobile/smart phones, email or social media channels to contact pupils or parents. Where there is a need for communication to be sent electronically, the Academy text messaging service (Groupcall Messenger), email or one of the Trust's social media accounts must be used. (See the E-Safety Procedure).
- Staff must not knowingly accept pupils as friends/followers on their personal social media accounts – personal communication could be considered inappropriate and unprofessional and makes staff highly vulnerable to allegations. (See the E-Safety Procedure). This is with the exception of legitimate personal relationships created independently of work which may include family members and, where there is a genuine need or the children of close friends.
- Staff must not use their personal mobile or any other personal device to record or take pictures of pupils. (See the E-Safety Procedure).
- Staff should not make defamatory remarks about the Trust or colleagues, pupils, parents, AAC members, Trustees or any individuals connected with the Trust or share anything that could potentially bring the Trust into disrepute, even in closed social media groups. Care should be taken to avoid using language which could be deemed as offensive to others on all social media platforms, including both the GAT and personal channels. (See the ICT Acceptable User Policy, Staff Code of Conduct and the Whistleblowing Policy).

  Nothing in this policy shall preclude members of staff from exercising their employee rights including, but not limited to, the right to participate in legal conduct and to report information relating to suspected wrongdoing or dangers at work (that is, to "blow the whistle"). However, we strongly encourage you to seek advice before reporting a concern to anyone external including making any disclosure by way of social media which is unlikely to qualify for protection under the law.
- Staff must restrict any comments made on their personal social media accounts to being personal only (i.e. not appearing as if they represent the Trust's views) - staff must not use them for making 'flame' messages about anyone or any other organisation. The use of the Trust's internet connections and social media to make hostile, harassing, defamatory or threatening comments may be treated as gross misconduct, and the employee(s) responsible will be dealt with as set out in the Trust Disciplinary Policy. (See the ICT Acceptable User Policy).

9. Monitoring, Review and Evaluation

The Trust reserves the right to withdraw or suspend a user's access to the social media accounts at any time, to allow further investigation, should the Trust deem the staff member to be in breach of the Trust's policies and procedures. Should this happen, the social media account login details will be changed and redistributed to the authorised users.

The Trust Social Media Policy and other associated policies and procedures are reviewed every two years or sooner, if required, due to a change in legislation. Trust policies and procedures are approved by Trustees and are subject to Trade's Union consultation.

Twitter, Facebook and YouTube user guides are available and all authorised users should familiarise themselves with these guides. Should further training be required, please contact the Marketing and Communications team.

10. Contact Information

marketing@greenwoodacademies.org