The Park Federation Academy Trust

Social Media Policy 2025

Version History

Version	Date	Status and Purpose	Changes overview
1	September 2019	Appendix A added	
2	July 2020	Periodic review	
3	July 2021	Periodic review	No changes
4	August 2022	Periodic review	Additional guidance in Appendix A
5	September 2023	Periodic review	No changes
6	February 2024	Periodic review	Introduction of Hannah Ball Academy
7	October 2025	Periodic Review	No changes

Approval

Signed by CEO and Federation Principal on behalf of the Board of Directors

Dr. Martin Young

Dr. Martin Young.

Date of approval August 2025
Date of review September 2026

Notes on Document Control

This document is the property of The Park Federation Academy Trust and its contents are confidential. It must not be reproduced, loaned or passed to a 3rd party without the permission of the authoriser.

It is controlled within the Park Federation Academy Trust Admin Server where the electronic master is held and can be accessed on a read only basis, subject to security permissions.

Users of the document are responsible for ensuring that they are working with the current version.

Paper or electronic copies may be taken for remote working etc. However, all paper copies or electronic copies not held within the Admin Server are uncontrolled.
Hence the footer 'DOCUMENT UNCONTROLLED WHEN PRINTED' which must not be changed.

Once issued, as a minimum this document shall be reviewed on an annual basis by the originating team/function. Any amendments shall be identified by a vertical line adjacent to the right hand margin.

To enable continuous improvement, all readers encouraged to notify the author of errors, omissions and any other form of feedback.

Contents

OPENING STATEMENT- principles this policy is based upon. 4
1.0 POLICY STATEMENT 4
1.1 Eligibility 5
1.2 Responsibility and Accountability 6
2.0 RECOMMENDATIONS and REQUIREMENTS FOR THE USE OF ONLINE SOCIAL NETWORKS 6
2.1 ICT equipment supplied to teachers and other staff for home use. 6
2.2 'Partners in Learning' 7
Appendix A - Guidance on use of Facebook, Instagram and Twitter 9

OPENING STATEMENT- principles this policy is based upon.

A common-sense approach should be taken when thinking of social media.

Underlying safeguarding principles must be adhered to. Rules to keep children safe and the sharing of information protocols within the Central Trust and our academies are important when dealing face to face with people, the same principles should again apply when posting anything onto the Internet.

In addition, we know we should be polite, professional and discrete when communicating with others in person in and out of the academy and so should be the same when communicating online.

Influence of Social Media heightens the need for staff to think through their actions even more carefully to avoid any areas of potential exploitation from others.

1.0 POLICY STATEMENT

The purpose of this Policy is to set out the Park Federation Academy Trust's recommendations and requirements for the use of social networking media by its staff members and volunteers.

In doing so, the Trust seeks to achieve an appropriate balance in the use of social networks by staff as private individuals, but also as employees and educators, with professional reputations and careers to maintain, and contractual and legislative requirements to adhere to.

The Trust does not wish to discourage staff from using such sites on the Internet in their personal time, however it does expect certain standards of conduct to be observed in order to protect the Trust and its reputation, and also to protect staff from the dangers of inappropriate use.

Accessing social media sites and personal email accounts, in working time and/or from Trust/Academy ICT equipment is strictly forbidden.

Policy scope

This policy applies to The Park Federation Academy Trust Members, Board Directors, Academy Council members, all teaching and other staff, external contractors providing services on behalf of the academy, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the Trust.

Legal Framework

The Park Federation Academy Trust is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the Trust are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- Human Rights Act 1998
- Common law duty of confidentiality, and
- Data Protection Act 2018.

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 2018.
- Information divulged in the expectation of confidentiality
- School business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and politically sensitive information.

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952, 1996 and 2013
- The Equality Act 2010
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988.

The Park Federation Academy Trust could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc. or who defame a third party while at work may render The Park Federation Academy Trust liable to the injured party.

Related Policies

This policy should be read in conjunction with the following Trust policies:

- Disciplinary Policy and Procedure
- ICT Policy/Agreement
- Child Protection Policy and any other policies related to safeguarding
- Whistleblowing Policy
- Bullying and Harassment Policy
- Code of Conduct

1.1 Eligibility

This policy largely relates to the use of social media applications by Trust staff in their own personal time, using their own ICT equipment. This is because using the Trust's equipment and or network to access such sites is prohibited.

Social media applications include, but are not limited to:

- Social Networking (e.g. Facebook, Instagram, Whats App, Snapchat, TikTok)
- Media sharing services, for example You Tube
- Micro-blogging applications (e.g. X or Threads)
- Online discussion forums and opinion sites (e.g. Ning)
- Blogs (e.g. Blogger, LiveJournal, Xanga)

1.2 Responsibility and Accountability

CEO/COO/Principal/Senior Leaders:

- Should ensure that all existing and new staff are familiar with this policy and its relationship to the Trust's standards, policies and guidance on the use of ICT.
- Should provide opportunities to discuss appropriate social media use by staff on a regular basis, and ensure that any queries raised are resolved swiftly.
- Must ensure that any allegations raised in respect of access to social media sites are investigated promptly and appropriately, in accordance with the Trust's Disciplinary Policy and Procedures

Employees:

- Should ensure that they are familiar with the contents of this policy and its relationship to the Trust's standards, policies and guidance on the use of ICT.
- Should raise any queries or areas of concern they have relating to the use of social media sites and interpretation of this Policy, with their senior lead in the first instance.
- Must comply with this policy where specific activities/conduct is prohibited.

Board of Directors

- Will review this policy and its application on an annual basis.
- Should ensure that their own conduct is in line with that expected of staff, as outlined in this policy.

2.0 RECOMMENDATIONS and REQUIREMENTS FOR THE USE OF ONLINE SOCIAL NETWORKS

Working in an educational setting with young people, staff have a professional image to uphold, and how individuals conduct themselves online, helps to determine this image.

2.1 ICT equipment supplied to teachers and other staff for home use.

Will be permitted to the use such equipment on their home network, supplied through an ISP - Internet Service Provider- whether wired or wireless (Wi-Fi) to access services such as the internet.

Friends/Befriending:

- One of the functions of social networks is the ability to "friend" others, creating a group of individuals who share personal news and /or interests. The Trust prohibits staff from accepting invitations to "friend" pupils, or pupil's family members/friends.
- Staff must not initiate friendships with pupils, or pupils' family members/friends, under any circumstances.
- Staff who maintain social media friendships with work colleagues, are required to adhere to the requirements below relating to content of interactions.

Content of interactions:

Staff must not make reference on social media sites to the Trust, its employees, pupils, and their families. If staff adhere to this recommendation then the personal content of an individual's social media memberships is unlikely to be of concern to the Trust.

If employment at the Trust is referred to, then the information posted would need to comply with the conditions set out below.

- Any references made to the Trust, its employees, pupils and their families, should comply with the Trust's policies on conduct/misconduct, equal opportunities, and bullying and harassment.
- Staff must not post information on a social media site which is confidential to the Trust, its employees, its pupils or their families.
- Staff must not post entries onto social media sites which are derogatory, defamatory, discriminatory or offensive in any way, or which could be perceived to and have the potential to bring the Trust into disrepute.
- Staff should not use the Trust logo on their own personal social media accounts, and should not post any photographic images that include **children**
  Any photographs posted with other members of staff must be with their permission and reflect and maintain a respected view of the Trust. They must not in any way bring the Trust into disrepute or provide the possibility of the Trust being brought into disrepute.
- Staff must not download copyrighted or confidential information.
- Staff must not express personal views which could be misinterpreted as those of the Trust

2.2 'Partners in Learning'

- When posting any information onto a social media site, staff must not post any entry that puts their effectiveness to perform their normal duties at risk.
- If individuals feel aggrieved about some aspect of their work or employment, there are appropriate informal and formal avenues, internally within the Trust, which allow staff to raise and progress such matters. Social networks are not the appropriate forum to raise such matters. Employees should discuss any concerns with their Principal or Line Manager in the first instance. Guidance is also available from HR and trade unions.

Security

Staff are advised to check their security profiles and privacy settings on the social networks that they use. If individuals are not clear about how to restrict access to their content, they should regard all content as publicly available and act accordingly.

In using social media sites, staff are recommended to only post content that they would wish to be in the public domain. **Even if content is subsequently removed from a site it may remain available and accessible**. Staff should consider not only how content could reflect on them, but also on their professionalism and the reputation of the Trust as their employer.

Even with privacy settings in place it is still possible that the personal details of staff may be accessed more broadly than the other networkers identified by them. Any reference to such information by pupils and/or their families, which a staff member deems to be inappropriate or is concerned about, should be reported to their Line Manager in the first instance.
If a member of staff becomes aware that a pupil (or group of pupils) has made inappropriate/insulting/threatening comments about them, or other staff members, on a social media site; then they must report this to the Principal so that the appropriate process can be followed.

Policy breaches:

Staff found to be in breach of this policy may be subject to disciplinary action, in accordance with the Trust's Disciplinary Policy and Procedures, with potential sanctions up to and including dismissal.

Information shared through social media sites, even on private spaces, is subject to copyright,

data protection, freedom of information, equality, safeguarding and other legislation.

Where staff work in roles that are governed by professional bodies/professional codes of conduct; the professional rules relating to social media applied to them may be more stringent that those within this Policy.

Whistleblowing

Where an employee releases information through Social Media that may be considered as a Public Interest Disclosure ('Whistle Blowing'), The Park Federation Academy Trusts Whistleblowing Policy shall be initiated in the first instance before any further action is taken.

ICT Monitoring

The Park Federation Academy Trust monitors usage of its Internet and email services without prior notification or authorisation from users. Users of the Academies email and Internet services should have no expectation of privacy in anything they create, store, send or receive using the Trust's ICT systems.

Don't accept friend requests from pupils on social media

Appendix A - Guidance on use of Facebook, Instagram and X (Formally known as Twitter)

10 rules for trust/academy staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the Principal about what's happening

A parent adds you on social media

- It is recommended that you do not respond. Bear in mind that:
- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Check your Facebook privacy settings

- Change the visibility of your posts and stories to 'Friends', rather than 'Public'. Otherwise pupils and their families may be able to see your posts and pictures you've been tagged in, even if you haven't accepted a friend request or they're not on Facebook
- Don't forget to check your old posts and photos – see Facebook's privacy support page for step by-step instructions on how to do this
- The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster
- Prevent search engines from indexing your profile so people can't search for you by name – see Facebook's step-by-step instructions
- Remember, some information is always public; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender
- Google your name to see what information about you is visible to the public

Check your Instagram privacy settings

- Change your profile visibility from the default 'Public' setting to 'Private'. Otherwise pupils and their families will be able to see your posts, reels, locations, and who you are following and are followed by. Go to the Instagram Help Centre for support with your privacy settings
- If a pupil or parent followed you before you changed your privacy settings, block them to prevent them seeing your posts
- Be careful about giving third-party apps or websites access to your Instagram account, and check app privileges in your phone to see if any apps currently have access. Sharing your information can put your account at risk and make you visible on search engines, even if you have set your account to 'Private'.
- Remember, some information is always public; your username, your bio and your profile picture
- Google your name to see what information about you is visible to the public

Check your X privacy settings

- If you have a Twitter account specifically for or about teaching, make sure you don't include identifying information about yourself or your trust/academy. Use a nickname, for example 'Miss M'
- Change the visibility on your birth date to 'You follow each other' to prevent pupils and parents seeing this personal information. See Twitter's profile visibility guidance for more support
- Remember, your username, biography, location, website and profile picture are always public and can be seen by pupils and parents, even if they don't follow you and you have protected your tweets
- Protect your tweets by checking the box in the 'Audience and tagging' section of your privacy settings. This will mean only your approved followers can see your tweets
- Google your name to see what information about you is visible to the public