

## Social Media (Employee) Policy

Policy Code:	HR22
Policy Start Date:	September 2017
Policy Review Date:	September 2020

Please read this policy in conjunction with the policies listed below:

- HR3 Grievance Procedure
- HR5 Acceptable Use Policy
- HR6 Data Protection Policy
- HR12 Staff Disciplinary Procedure
- SW5 Safeguarding (Child Protection) Policy
- Trust Code of Conduct

---

## **1 Policy Statement**

Social media technology can serve as a powerful tool to enhance education, communication and learning. This technology can provide both educational and professional benefits. This policy is in place to minimise the risk to The Trust through use of social media, whilst recognising any benefits its use may present.

## **2 Roles, Responsibilities and Implementation**

- 2.1 The Pay, Performance and HR Committee has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. This committee delegates day-to-day responsibility for operating the policy and ensuring its maintenance and review to the Head of Human Resources.
- 2.2 Leaders and Managers have a specific responsibility to ensure the fair application of this policy and all employees are responsible for supporting colleagues and ensuring its success.

## **3 Aims**

- 3.1 To ensure that all employees, trustees and governors adhere to this policy. The Trust is committed to ensuring that all stakeholders who utilise social media technology for professional purposes described below, including staff and students, do so in a safe and responsible manner.
- 3.2 To ensure all employees, students, trustees and governors follow the guidelines and recommended practices for professional social media communication between staff, as well as social media communication between staff and students.
- 3.3 To ensure The Trust recognises the public and pervasive nature of social media communications, as well as the fact that in this digital era, the lines between professional and personal endeavours are sometimes blurred. All employees, trustees and governors should also follow the guidelines and recommended practices for use of personal social media by staff.

## **4 Definition of Social Media**

- 4.2 Social media are defined as any form of online publication or presence that allows interactive communication, including, but not limited to, social networks, blogs, Internet websites, Internet forums, and wikis. Examples of social media include, but are not limited to, Facebook, Twitter, YouTube, Google+, and Flickr.

---

**Professional social media** is a work-related social media activity that is either school-based (e.g., a Facebook page for an Academy or a teacher establishing a blog for his/her class), or non-school-based (e.g. a twitter account to promote a Trust service).

**Personal social media** use is a non work-related social media activity (e.g. an employee establishing a Facebook page or a Twitter account for his/her own personal use).

## **5 Maintaining Separate Professional and Personal E-mail Accounts**

- 5.1 Employees who decide to engage in professional social media activities should maintain separate professional and personal e-mail addresses. As such, employees should not use their personal e-mail address for professional social media activities; rather, they should use a professional e-mail address that is completely separate from any personal social media they maintain.

## **6 Communication with Students**

- 6.1 Employees who work with students and communicate with them through professional social media sites should follow these guidelines:
- (a) Professional social media sites that are Academy-based should be designed to address reasonable instructional, educational or extra-curricular programme matters.
  - (b) Each Academy keeps a file of active professional social media accounts and what they are used for.

## **7 Guidance Regarding Professional Social Media Sites**

- 7.1 Employees should treat professional social media space and communication like a classroom and/or a professional workplace. The same standards expected in professional settings are expected on professional social media sites. If a particular type of behaviour is inappropriate in the classroom or a professional workplace, then that behaviour is also inappropriate on the professional social media site.
- 7.2 Employees should exercise caution, sound judgment and common sense when using professional social media sites.
- 7.3 When establishing professional social media sites, employees should consider the intended audience for the site. Employees must also consider the level of privacy assigned to the site; specifically whether the site should be a private network (e.g. it is limited to a particular class or particular grade within a school)

---

or a public network (e.g. anyone within the school, a larger group). It is recommended practice for professional social media sites to be private networks, unless there is a specific educational need for the site to be a public network.

- 7.4 Employees should obtain Academy SLT approval by using a registration form before setting up a professional social media presence. These forms can be obtained from the Federation's Strategic ICT Co-ordinator.
- 7.5 A list should be maintained of all professional social media accounts within the Academy.
- 7.6 Professional social media sites should include language identifying the sites as professional social media sites to differentiate them from personal sites.
- 7.7 Employees should use privacy settings to control access to their professional social media sites with the objective that professional social media communications only reach the intended audience. However, employees must be aware that there are limitations to privacy settings. Private communication published on the Internet can easily become public. Furthermore, social media sites can change an employee's current default privacy settings and other functions. As a result, each employee has a responsibility to understand the rules of the social media site being utilised.
- 7.8 Professional social media communication must remain legal. Confidential information must not be disclosed and prohibitions must be placed on the use of harassing, obscene, discriminatory, defamatory or threatening language.

If images of students are to be posted online, there must be a media consent form on file at the Academy for each child featured. This form can be obtained from the data team at each site. It is not recommended that employees post photos of colleagues on professional social media sites without prior permission of the employee in the photo.

- 7.9 Employees are responsible for monitoring and providing feedback regarding their work-related professional social media sites. The monitoring responsibilities include reviewing the professional social media sites on a regular basis. If managers discover questionable communications or behaviour on professional social media sites, they are required to contact a member of the SLT for assistance. If employees decide to create a professional social media site and they are notified of questionable communications or behaviour on their site, they may remove the material and/or contact SLT.

---

## **8 Personal Social Media Use**

8.1 In order to maintain a professional and appropriate relationship with students, employees should not communicate with or have any direct connection with students who are currently enrolled in any of The Trust's Academies on personal social media sites. Employee communication with students may be permitted in the following circumstances:

- (a) communication with parents or carers of students, where the communication does not relate to any student enrolled on any of the Trust's Academies.;
- (b) if an emergency situation requires such communication, in which case, the employee should notify SLT of the communication as soon as possible; and
- (c) if the student is an existing friend of familial relation of the employee, subject to the approval of the SLT, such approval at the absolute discretion of the SLT

## **9 Guidance Regarding Personal Social Media Sites**

9.1 Staff should exercise caution and common sense when using personal social media sites:

- (a) As a recommended practice, employees are encouraged to use appropriate privacy settings to control access to their personal social media sites. However, employees must be aware that there are limitations to privacy settings. Private communication published on the Internet can easily become public. Furthermore, social media sites can change an employee's current default privacy settings and other functions. As a result, employees are responsible for understanding the rules of the social media site being utilised.
- (b) It is not recommended that employees "tag" photos of their colleagues, volunteers, contractors or vendors without the prior permission of the individuals being tagged.
- (c) Personal social media use, including out of hours use, has the potential to result in disruption at the Academy or within The Trust as a whole.
- (d) Employees are prohibited from posting or disclosing personally identifiable student information or confidential information via personal social media sites.

- 
- (e) Employees should not use any of Academies' or Trust logos or make representations that their personal social media sites speak in an official capacity. Employees should make it clear in personal social media postings, or in their personal profiles, that they are speaking on their own behalf. Employees should write in the first person and use a personal email address.
  - (f) If Employees see social media content that disparages or reflects poorly on The Trust, they should contact their Academy SLT.
  - (g) Employees should not use personal social media to participate in any form of cyberbullying (bullying, harassment or victimisation) of colleagues, volunteers, contractors or vendors, Any reported cases of cyberbullying will be investigated through the Trust's Disciplinary policy.

## **10 Applicability of Policies and Other Laws**

10.1 This policy provides guidance intended to supplement, not supersede, existing child protection procedures and laws, the Acceptable Use, Code of Conduct and Data Protection Policies.

## **11 Social Media Misuse**

- 11.1 Breaches of this policy may lead to disciplinary action including dismissal. Any employee suspected of committing a breach of this policy will be required to cooperate with the Trust's investigation which may involve handing over relevant passwords and login details.
- 11.2 Employees may be required to remove any social media that the Trust considers to be a breach of this policy. Failure to comply with such a request may result in disciplinary action.
- 11.3 Employees must avoid making any social media communications that could damage The Trust's business interests or reputation, even indirectly.
- 11.4 Employees must not use social media to defame or disparage the Trust, its employees or any third party, to harass, bully or unlawfully discriminate against staff or third parties, to make false or misleading statements, or to impersonate colleagues or third parties.
- 11.5 Employees must not post comments about sensitive business-related topics, such as the Trust's performance, or do anything to jeopardise the Trust's

---

confidential information or intellectual property unless authorised to do so and only on professional social media.

- 11.6 Employees must not post any communications which would amount to a breach of any of the Trust policies.

## **12 Monitoring**

- 12.1 To ensure that Trust policies are being complied with and for legitimate business purposes, the Trust reserves the right to monitor, intercept and review, without further notice, staff activities using Trust IT resources and communications systems. This includes, but is not limited, to social media postings and activities. Employees consent to such monitoring by their use of such resources and systems.

## **13 Recruitment**

- 13.1 The Trust may use internet searches to perform due diligence on candidates in the course of recruitment. When this occurs, The Trust will act in accordance with its Data Protection and Equal Opportunities obligations.

## **14 Policy Change**

This policy may only be amended or withdrawn by The Priory Federation of Academies Trust.

---

## **Appendix 1 - Key Terms**

**Blogs** - Short for 'web-logs', these are sites that can function as on-going journals with multiple entries. Typically, entries are categorized with 'tags' (content labels or captions) for easy searching. Most blogs allow for reader comments. Examples: Blogger, Wordpress, TypePad.

**Micro-Blogs** - These blogs allow for shorter content posts, typically with a limited set of typed characters allowed. Micro-blogs can be used for status updates and to quickly communicate information to 'friends' or 'followers.' Examples: Twitter, Tumblr.

**Networking** - These sites allow people to connect with each other around common interests, pursuits and other categories. Examples: Facebook, LinkedIn, Google+, Ning, StumbleUpon

**Photo/Video** - These sites allow people to share videos, images, slideshows, and other media. Often these sites allow viewers to comment and share posted content. Examples: YouTube, Vimeo, Flickr.





# **The Priory Federation of Academies Trust**

## **Social Media (Employee) Policy**

This Policy has been approved by the Pay, Performance and HR Committee:

Signed..... Name..... Date:

Trustee

Signed..... Name..... Date:

Chief Executive Officer

Signed..... Name..... Date:

Designated Member of Staff

Please note that a signed copy of this agreement is available via Human Resources.