Policy A2 – Use of Social Media

University of Brighton Academies Trust

1. Introduction

1.1 The Trust recognises and embraces the numerous benefits and opportunities that social media offers. While employees are encouraged to engage, collaborate, and innovate through social media, they should also be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation.

2. Scope

2.1 The purpose of this policy is to encourage good practice, to protect the Trust and its employees, and to promote the effective use of social media as part of the Trust activities.

2.2 This policy covers personal and professional use of social media and aims to encourage its safe use by the academies and its employees.

2.3 The policy applies regardless of whether social media is accessed using the Trust's ICT facilities and equipment, or equipment belonging to members of staff.

2.4 Personal communications via social media accounts that are likely to have a negative impact on professional standards or the Trust's reputation are within the scope of this policy.

2.5 This policy covers all individuals working at all levels and grades, including full-time and part-time employees, fixed-term employees, and agency workers. The use of Trust or academies within this policy is interchangeable.

3. Roles, responsibilities, and procedure

3.1 Employees should:

- be aware of their online reputation and recognise that their online activity can be seen by others including parents, pupils, and colleagues on social media
- ensure that any use of social media is carried out in line with this policy and other relevant policies
- be aware that any excessive use of social media in academies may result in disciplinary action
- be aware that they should not set up academy, class, or subject-specific social media channels without authorisation from the Marketing and Communications team
- 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 on a social networking site is something that they want pupils, colleagues, other employees of the Trust, or even future employers, to read. If in doubt, don't post it!

3.2 Principals and Heads of Professional Services are responsible for:

- addressing any concerns or questions employees may have on the use of social media and should liaise with the Marketing and Communications when in doubt
- discuss the need for a social media channel or account with the Head of Marketing and Communications for review and sign off
- operating within the boundaries of this policy and ensuring that all staff understand the standards of behaviour expected of them

- identifying colleagues who will be responsible for managing daily content activity.

3.3 Marketing and Communications team are responsible for:

- implementing and reviewing this policy
- administering all social media accounts
- holding a central record of all accounts, the login and editor details
- support or take control of academy accounts during a crisis or major incident
- support academies during difficult and persistent interactions with pupils, parents, or other external stakeholders.

4. Definition of social media

4.1 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, Twitter, Google+, Instagram, Myspace, Flickr, and YouTube.

5. Acceptable use

5.1 Employees should be aware that the following social media platforms have been approved. Social media platforms not listed are prohibited.

- Facebook
- Twitter
- YouTube
- Instagram

Academies are limited to one account on each approved platform. Additional accounts are to be reviewed and signed off by the Head of Marketing and Communications.

5.2 Employees should be aware that content uploaded to social media is not private. Even if access is restricted to 'friends', there is still capacity for it to be re-posted or distributed beyond the intended recipients. Therefore, employees using social media should conduct themselves with professionalism and respect.

5.3 Employees should be aware of both professional and social boundaries and should not, therefore, accept or invite 'friend' requests from pupils or ex-pupils under the age of 18, or from parents on their personal social media accounts such as Facebook. All communication with parents via social media should be through the academy or Trust's social media accounts. Employees should note that the use of social media accounts during lesson time is not permitted.

5.4 Employees should:

- maintain a professional persona through any use of social media for work purposes including the consideration of the type of profile picture used. This should be a professional/smart image to aid colleagues and students in identifying you and this should be a head and shoulders picture with a neutral background.
- be mindful of the content they are sharing.
- seek advice from their principal or manager if unsure whether content is suitable before posting.
- use formal usernames to identify themselves on social media (e.g. @MrSmith_TBHA).
- ensure that they set the privacy levels of their personal sites to be as strict as possible and to opt out of public listings on social networking sites to protect their own privacy.

5.5 Employees should not upload any content on to social media sites that:

- is confidential to the Trust, academy, or its staff
- amounts to bullying
- amounts to unlawful discrimination, harassment, or victimisation
- brings the Trust or academy into disrepute
- contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images, or video clips
- undermines the reputation of the academy and/or individuals
- is defamatory or knowingly false
- breaches copyright
- is in any other way unlawful

5.6 Employees should not:

- Use avatars or photos of a social nature as profile pictures
- Initiate contact with former students on leaving the employment of the academy or Trust
- put themselves in a position where extreme political, religious, or philosophical views expressed via social media conflict with those of a public institution such as an academy
- use social media to communicate with students, they can only do so through the Learning Platform of the academy. No other service is to be used unless a pedagogical business case and associated risk assessment is agreed by the Head of ICT Services
- Use academy and Trust email addresses and other official contact details when setting up personal social media accounts or to communicate through such media
- have contact through any personal social medium with any student or member of a students' family, whether from an academy or any other school, unless the students are family members
- use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations the academy or the Trust

6. Safeguarding

6.1 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
- encouraging violent behaviour, self-harm or risk-taking.

In order to mitigate these risks, there are steps that can be taken to promote safety online:

- Information should not be used in an attempt to locate or meet a child
- Ensure that any messages, photos, or information comply with existing policies

6.2 Reporting safeguarding concerns

- Any content or online activity which raises a safeguarding concern must be reported to the Academy Designated Safeguarding Lead
- Any online concerns should be reported as soon as identified as urgent steps may need to be taken to support the child
- With regard to personal safeguarding, any harassment or abuse received online while using work accounts must be reported to the line manager

6.3 Reporting, responding, and recording cyberbullying incidents

- Staff should never engage with cyberbullying incidents. If an employee discover a website containing inaccurate, inappropriate or inflammatory written material relating to themselves, or images which have been taken and/or which are being used without permission, it must immediately be reported to the relevant line manager
- Staff should 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.

6.4 Action by employer: inappropriate use of social media

- Following a report of inappropriate use of social media, an investigation will be conducted promptly
- If in the course of the investigation, it is found that a pupil submitted the material to the website, that pupil will be disciplined in line with the academy behaviour policy
- The investigating manager, where appropriate, will approach the website hosts to ensure 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 academy will give their full support and assistance
- Checks will be carried out to ensure that the requested amendments or removals are made. If the website(s) does not co-operate, the investigating manager will contact the internet service provider (ISP) as the ISP has the ability to block access to certain sites and, in exceptional circumstances, can close down a website
- If the material 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.

7. Breaches of this policy

7.1 Any member of staff suspected of committing a 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 Trust's bullying or disciplinary procedure. The member of staff will be expected to co-operate with the Trust's investigation which may involve:

- handing over relevant passwords and login details
- printing a copy or obtaining a screenshot of the alleged unacceptable content
- determining that the responsibility or source of the content was in fact the member of staff.

7.2 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 Trust or the individuals concerned. Employees should 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. Where conduct is considered to be unlawful, the academy will report the matter to the police and other external agencies.

8. Monitoring and review

8.1 If a principal/Head of Service reasonably believes that an employee has breached this policy, from time to time the Trust will monitor or record communications that are sent or received from within the school/trust's network.

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

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

8.3 This policy does not form part of any employee's contract of employment and may also, after consultation with the trade unions, be amended from time to time by the Trust.

9. Legislation

9.1 Acceptable use of social networking must comply with UK law. In applying this policy, the 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

9.2 The internet is a fast-moving technology, and it is impossible to cover all circumstances or emerging media – the principles set out in this policy must be followed irrespective of the medium. When using social media, employees should be aware of the potential impact on themselves and the employer, whether for work-related or personal use; whether during working hours or otherwise; or whether social media is accessed using the employer's equipment or using the employee's equipment. Employees should use discretion and common sense when engaging in online communication.

10. Policy and status review

Written by:	Head of Marketing and Communications
Owner:	Head of Marketing and Communications
Status:	V1 = Approved V2 = Approved
Summary of changes	V2 = Amendment made to add guidance on use of profile pictures
Approval date:	V1 = 30.11.2020 Finance and Resources Committee V2 = Chair of FRC 26-02-2021
Review date:	November 2021