Policy A2 – Use of Social Media

University of Brighton Academies Trust

1. Introduction

1.1 The Internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as *Facebook* to keeping up with other people's lives on *Twitter* and maintaining pages on Internet encyclopedias such as *Wikipedia*.

1.2 While recognising the benefits of these media as new opportunities for communication, this policy sets out the principles that University of Brighton Academies Trust staff and contractors are expected to follow when using social media.

1.3 It is crucial that students, parents and the public at large have confidence in the decisions and services of the Trust. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of students and other staff and the reputation of the Trust and its Sponsors are safeguarded.

1.4 This policy also aims to help staff use social media with minimal professional risk. Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

2. Scope

2.1 This policy applies to all teaching and other staff, whether employed directly by the Trust, external contractors providing services on behalf of the Trust, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the Trust. These individuals are collectively referred to as 'staff members' in this policy.

2.1 This policy covers personal use of social media as well as the use of social media for official Trust or academy purposes, including sites hosted and maintained on behalf of the Academies.

2.3 This policy applies to personal web presences such as social networking sites (for example *Facebook*) blogs and microblogs (such as *Twitter)*, chatrooms, forums, podcasts, open access online encyclopedias (such as *Wikipedia*), social bookmarking sites (such as *del.icio.us*) and content sharing sites (such as *flickr* and *YouTube*). 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.

2.4 This policy applies to all sites however, where applicable, the individual sites may append additional guidelines to this policy based on a specific individual need or requirement. Therefore this would become non-exhaustive policy and we recommend that you check with your establishment directly to obtain the complete policy set applicable to you.

3. Professional use of Social Media

3.1 Professional use - Introduction

3.1.1 The Trust maintains a presence on various social media sites as they provide very effective additional channels of communication with parents/carers, students and the wider community.

3.1.2 For example, Twitter is used to collate and publicise a stream of positive messages about the multitude of activities that go on at each academy every day. Some staff have chosen to play a part in this use of social media for professional purposes, often to highlight successes and to encourage participation in their area of work. This is not without risk, however and staff members should be aware that;

- Services such as Twitter are in the public domain and are regularly used by journalists, students, parents and employers
- Submissions can take on a life of their own once sent by users, who should not rely on being able to delete them
- An academy may re-tweet the submissions of staff members to their wider following

3.2 Professional Use - Policy statements

3.2.1 Staff members must not upload video content to hosting services (such as YouTube) without authorisation from a senior leader such as the principal or the Head of ICT Services. This is for reasons of safeguarding and for maintaining the reputation of the academy. Likewise, staff members must not make use of any social media service with students apart from the Learning Platform of the academy, unless a pedagogical business case and associated risk assessment is agreed by a senior leader and the Head of ICT Services.

3.2.2 Staff members should maintain a professional persona through any use of social media for work purposes. User names should be formal (e.g. @MrSmith_AcademyName) or anonymised (e.g. @PE_WSL). The latter option also distances the user from their real life identify and makes online bullying less likely.

3.2.3 All professional submissions to social media sites must show the academy in a positive light and should be written without ambiguity or any rhetorical device (such as sarcasm) which might be misinterpreted. It is surprisingly easy for even the gentlest of humour to be read differently than intended when parsed through abbreviated media such as Twitter.

3.2.4 Staff members must not enter into dialogue using social media such as Twitter, which each academy uses purely as a one-way channel for distributing news. Any attempt by other users to interact with staff members via such services should be reported to the head of ICT Services for advice and resolution. The simplest option is usually to take such issues offline.

3.2.5 Staff members should exercise professional judgement when using social media. It is good practice to ask a senior colleague's opinion before posting an update to a social media service. If in doubt over the appropriateness of a submission, the best option is not to make it. Appropriate disciplinary action will be taken should a member of staff make a submission which brings an academy or the Trust into disrepute.

3.2.6 Any images submitted to a social media site should be chosen carefully and should show the academy positively. Images of students must only be uploaded with exceptional

caution; no individual or close up images should be used where the student could be identified. Likewise, no image which might reasonably be judged to cause embarrassment to the student should be published. 'Over the shoulder' images (where individuals are not recognisable) or group shots of 3 or more students are safest. Staff should seek advice from a senior colleague before publishing images of students wearing PE kit.

3.2.7 Individual students should not be identifiable through submissions to social media sites, for safeguarding reasons. For example, "Excellent piece of Level 7 work shown here by Tom in Y8" is acceptable, whereas including Tom's surname is not. Any submission that includes an image of a student must not make reference to the student's first, sur- or full name under any circumstances.

3.2.8 Strong password security must be maintained and regularly changed for any social media account, to prevent it from being hi-jacked and misused. Passwords should never be written down. A combination of upper and lower case characters should be combined with numerals. The potential for hi-jacked accounts to bring an academy or the Trust into disrepute is significant and responsibility for account security lies with the staff member who controls it.

4. Personal use of Social Media

4.1 Personal use - Introduction

4.1.1 It is reasonable for members of staff to maintain personal web presences in their lives. Indeed, in 2014 over 72% of Internet users have a Facebook account.

4.1.2 Teachers, however, occupy an almost unique professional position due to their work with children and the moral credibility they must maintain. There have been several recent cases where teachers have suffered serious professional consequences as a result of poor judgment in the use of social media.

4.1.3 It is worth considering that information (text, images, and video) held in web presences;

- Is never completely private and can very easily enter the public domain,
- Can be misinterpreted and taken out of context by audiences it was not originally intended for,
- May persist for a timeframe beyond your wishes,
- Might be copied and used by third parties without your consent,

4.1.4 It is therefore vital that use of social media in the personal lives of staff be totally separated from their professional identity. However, staff should be aware that even if this separation is strictly adhered to, it remains relatively easy for people (students, journalists, future employers etc.) to connect academy staff with 'private' social media presences.

4.2 Personal Use: Additional Policy statements

4.2.1 Staff members must not identify themselves as employees of an academy or the Trust in their personal web presences or purport to represent an academy or Trust view. This is to prevent information on these sites from being linked with the academy or Trust and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services. Do not name an academy or Trust in any biographical detail associated with personal accounts or use an academy or trust logo or any other identifying information (such as location).

4.2.2 Staff members must not 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.

4.2.3 Staff members should not 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. Even if separation of professional and private lives has been maintained, recent case history shows that teachers who express such views have found their position at an academy to be untenable.

4.2.4 Staff members should not use social media to document or distribute evidence of activities in their private lives that may bring an academy or the Trust into disrepute. Even if separation of professional and private lives has been maintained, recent case history shows that teachers whose behaviour becomes known through social media have found their position at an academy to be compromised.

4.2.5 If staff members wish to use the affordances of social media 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.

4.2.6 Staff members must decline 'friend requests' from students they receive in their personal social media accounts. Instead, if they receive such requests from students who are not family members, they must discuss these in general terms in class and signpost students to become 'friends' of the official academy Facebook or Twitter accounts.

4.2.7 On leaving the employment of the academy or Trust, staff members must not initiate contact with former students.

4.2.8 Information staff members have access to as part of their employment, including personal information about students and their family members, colleagues and other parties must not be discussed on their personal web presence.

4.2.9 Academy and Trust email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

4.2.10 Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity from work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

4.2.11 Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.

4.2.12 Staff members must not 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.

4.2.13 Staff members are strongly advised to 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. Breaches of policy

5.1 Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with the Trust Disciplinary Policy. A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of an academy or the Trust or any illegal acts or acts that render an academy or the Trust liable to third parties will result in disciplinary action appropriate to the severity of the breach.

5.2 Contracted providers of services to an academy or the Trust must inform the academy or Trust immediately of any breaches of this policy by their staff so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the academy or Trust. Any action against breaches should be according to contractors' internal disciplinary procedures.

6. Legal Framework/s

6.1 Each academy and the Trust are 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:

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

6.2 Confidential or sensitive information includes, but is not limited to:

- Person-identifiable information, e.g. student and employee records protected by the Data Protection Act 1998,
- Information divulged with the expectation of confidentiality,
- Trust or County Council 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.

6.3 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 and 1996
- 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.

6.4 The 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 Trust liable to the injured party.

7. Policy status and review

Written by:	ICT Director
Owner:	ICT Director
Status:	Approved
Approval date:	UoBAT – Board of Directors 10/12/15 HAT – Board of Directors 17/12/15 Merger editorial changes 1 September 2017
Review Date:	2019/20