Title	Social Media
Associated Policies	• Professional and Safe Conduct (TPO/STA/10) • Disciplinary Procedure (TPO/STA/22) • Safeguarding and Child Protection (TPO/HS/05)

REVIEWED: AUGUST 2016 NEXT REVIEW: AUGUST 2019

1. Policy Statement

1.1 The primary purpose of the Personal Use of Social Media Sites Policy and procedure is to clarify for Trust staff/governors how they should conduct themselves when using all forms of social media sites. If followed, it will help minimise risk in terms of safeguarding concerns or incidents where Trust staff/governors' integrity could be undermined, the school be brought into disrepute and professional relationships with colleagues and students compromised.

1.2 Additionally, adhering to the policy reduces the risk of employees/governors inadvertently contravening sections of the Data Protection Act or falling foul of libel, defamation and copyright laws.

1.3 This Policy does not form part of any employee's contract of employment and is entirely non-contractual. It may be amended, withdrawn, suspended or departed from at the discretion of the Trust.

2. Who does this policy apply to?

2.1 The policy is recommended for all Trust employees/governors. The policy is concerned with the personal use of social media sites, not with work/official social media sites. Any Trust staff wanting to create a work-related social media site must discuss this with and obtain approval from the CEO.

2.2 This policy should be read in conjunction with the Trust's Acceptable Use policy.

3. Who is responsible for carrying out this policy?

3.1 Principals should ensure that all academy staff and governors are aware of the Social Media policy and procedure and of their responsibilities under it. It is the responsibility of the Principal to ensure that breaches of the policy are investigated and addressed.

3.2 Staff and governors are expected to adhere to the policy and procedure and ensure that they conduct themselves in a manner that will not place students or vulnerable adults at risk, bring the school into disrepute or damage their own professional reputation.

3.3 The implementation of this policy will be monitored by the Senior Leadership Team and the governors of the Academy and will remain under constant review by Brooke Weston Trust.

4. What are the principles behind this policy?

4.1 Brooke Weston Trust's commitment to equality of opportunity will be observed at all times during the operation of this procedure. This will ensure that everyone concerned is treated fairly and without discrimination on the grounds of race, nationality, ethnic or national origins, gender, marital status, disability, age, sexual orientation, trade union membership or activity, political or religious belief and unrelated criminal conviction.

4.2 This policy is not intended to make Trust staff and governors aware of the risks they could face when sharing information about their personal/professional life.

4.3 Staff/governors should be encouraged to report any concerns that they have regarding content placed on social media sites to their Academy Principal.

5. Social media sites covered

5.1 This procedure covers all types of social media sites, which include but are not limited to:

- Social networking sites e.g. Facebook, Instagram, Snapchat
- Blogging
- Micro blogging sites e.g. Twitter
- Video clips and podcasts e.g. You Tube
- Discussion forums

6. Responsibilities of employees/governors

6.1 Trust staff/governors are personally responsible for the content they publish on social media sites.

6.2 Staff/governors should not accept students as "friends" and information must not be posted that would disclose the identity of students.

6.3 Students must not be discussed on social media sites.

6.4 Photographs or videos of students or their homes must not be posted on social media sites.

6.5 Staff/governors must not post information on sites, (e.g. photographs and videos), that could bring the school into disrepute.

6.6 Staff/governors must not represent their own views/opinions as being those of the school or the Brooke Weston Trust.

6.7 Potentially defamatory remarks towards the school, the Trust, staff, governors, students, students' relatives, partner organisations etc. must not be posted on social media sites.

6.8 Staff/governors must observe the requirements of the Equality Act and the Human Rights Act and must not use any offensive or discriminatory language on social media sites.

6.9 Staff/governors must not divulge any information that is confidential to the Academy, Trust or a partner organisation.

7. Security

7.1 Staff/governors should be mindful when placing information on social media sites that it is potentially visible to a large audience and could identify where they work and with whom, thereby increasing the opportunity for false allegations and threats. In addition it may be possible through social media sites for children or vulnerable adults to be identified, which could have implications for their security.

7.2 Furthermore, there is scope for causing offence or unintentionally causing embarrassment, for example if students find photographs of their teachers which may cause embarrassment and/or damage to their professional reputation and that of the Academy/Trust. In addition, it may be possible for other social media site users to identify where staff/governors live, which could have implications for individual security.

7.3 Therefore the utmost consideration should be given to the information posted on social media sites and staff/governors are advised to use appropriate security settings on such sites in order to assist in limiting the concerns above. See guidelines at Appendix One.

8. Employee group/networks

8.1 Employee groups should not be created on social media sites such as Facebook.

9. Disciplinary action

9.1 Staff should be aware that the use of social media sites in a manner contrary to this policy may result in disciplinary action.

9.2 As with all personal internet use, staff/governors using social media sites must not access social media sites for personal reasons during working time.

9.3 Any instances of cyber bullying will initially be addressed under the existing disciplinary procedures and may result in disciplinary action.

10. Disputes with third parties

10.1 In the event that a dispute with a third party or parent is initiated or perpetuated by means of social media this must be reported to the school's Executive Principal as soon as possible. No response to any post should be made until directed to do so.

10.2 The Executive Principal will consult with the Trust Director of IT and the Chief Executive who will decide what the response (if any) should be or whether to refer the matter to the Trust's legal advice team.

10.3 No conversation about any matter of complaint or dispute should be initiated by members of staff via any social media channel. They should instead refer the issue to the relevant senior member of staff and /or relevant school policies.

11. Policy Review

11.1 This policy will be monitored as part of the Academy's annual internal review and reviewed on a three year cycle.

APPENDIX 1 – GUIDELINES

1. Introduction

At the time of writing, there are over one billion Facebook users around the world, making it the most popular social networking site. However, the use of social media sites like Facebook carries a great deal of risk. For example, Facebook profiles can often contain names, addresses and dates of birth. This can lead to anyone being able to set up a credit card in your name. Also, identity thieves would find it easier to piece together information about you from different websites/resources and use it to their advantage. This sounds unlikely but it is a real risk: the Press often carries stories about people who have lost money or had their credit rating damaged, which can be very tedious to correct. Many employees/governors are registered onto Facebook or similar websites such as Twitter, Instagram and Snapchat. This guidance has been produced to help you, as an employee/governor, ensure that correct privacy settings have been enabled within your Facebook profile. For other social networking sites, the same rules and risks apply in principle, so you are advised to become aware of what privacy settings are built into the site and take time to change the default settings.

2. Scope

This guidance document relates to all social networking websites including, but not limited to, Facebook, Instagram, Twitter and Snapchat. This document is not intended to encourage the use of Facebook or similar social networking sites, but rather to ensure that employees/governors who use these websites are doing so safely.

3. Risks

There are many risks with using Facebook. Here are some risks that you need to be aware of:

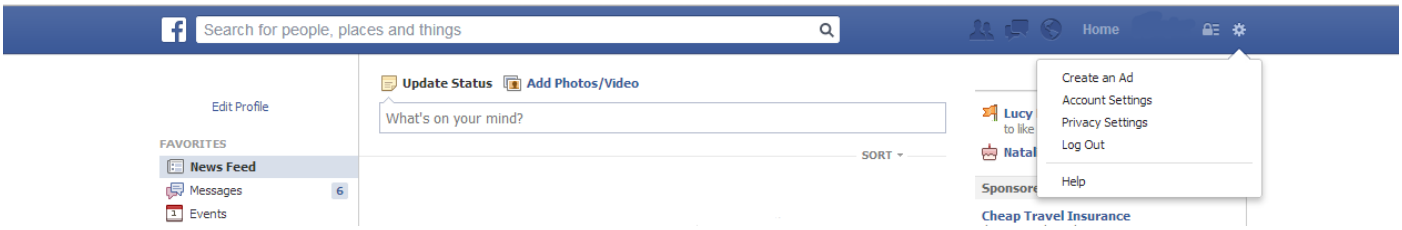
- Anyone could find out information about you through the use of Facebook
- Threatening messages could easily be sent through the use of Facebook
- Risks to professionalism and independence when working with children and vulnerable service users
- Information posted within the status field could possibly tell everyone that you are on holiday and your house will be empty for a couple of weeks
- Risk to children who update their status to show their whereabouts
- Possible damage to the school's reputation by posting inappropriate comments on another user's profile, which could be visible to everyone
- Inappropriate photographs or offensive jokes posted on an employee's profile

4. Facebook Privacy Overview

Facebook security is divided into separate parts: (see figure 1)

- Account Settings – To controls username/password details and to control what information you share with others.
- Privacy Settings - Security settings within the website to control what information is visible on your profile e.g. basic information, personal information, photos, wall posts and searching.

Figure 1



If you have entered your date of birth within your profile, change the privacy settings to display just the day and not the year.

Do not mention your mother's maiden name, your favourite pet or your school history in your profile. These are the security questions web sites such as banks use as part of checking who you are or in their "forgot password" functions. Although we recommend that you don't, some people use pet names and mother's maiden names as passwords, so by making this information available on your profile you may potentially be making it easier for people to hack your account.

If entering information or photos onto your profile, always bear in mind that a present or future employer could be viewing your profile.

Facebook provides every user with their own message board, also known as their "wall". The messages sent or received on your wall are displayed on your profile. Be careful about what is written on your wall and on your current status field, because others will be able to view the exchange of messages between you and your contact unless you secure your privacy settings (see Section 6 below for more information about privacy settings).

Examples of messages on user's wall which can be seen as a risk include:

- Telling your friends that you are going on holiday with the whole family – burglars would know there is an empty house and possibly your return date
- Inviting your friends to a house party – this could lead to strangers inviting themselves along – this happened on a Facebook profile where a group of strangers turned up and caused thousands of pounds worth of damage to someone's house

5.2 Accepting friend requests

Facebook encourages us to be friends with as many people as possible therefore some people may have a tendency to accept any friend requests they receive. As a Facebook user, you are advised to consider the following before accepting a friend's request:

- Think carefully about who you allow as a friend
- Remember people may not be who they say they are
- If in doubt of a person's identity, do not accept the request

6. Security/privacy settings within the website

Facebook offers a wide range of privacy settings to control who you share your information with, but it is up to you to ensure that these controls are set at an appropriate level. It is important to explore all the options under the privacy heading and amend the ones you feel are relevant. When using any social networking website, never use the standard default privacy settings, as these are more likely to leave your account open for other users to view.

This section gives you further details of the main privacy settings available on Facebook and how they can help you control the way you share your information. Make time to view them all and decide on what level you wish to set them.

6.1 Profile

By default Facebook allows all your friends and networks (e.g. groups) to view your profile information. Networks can contain many thousands of people so you will be leaving your information visible to these users if you keep this on the default setting.

Facebook allows users to secure your profile using the privacy settings. There are three settings to choose from:

- Making your profile available to everyone. This will make your profile available to everyone and anyone. This is not recommended.
- Making your profile available to your friends and networks. This setting allows all your friends and networks to view your profile. Friends are usually the contacts that you have created/received a request from and will only appear on your contacts list when both users have clicked "accept". Your profile would be open to anyone else within your network, i.e. all the groups/networks that you have joined. Again this opens your profile to anyone else that's listed as a member.

- Making your profile available to your friends only. This is the most secure option and is recommended. Other people can still search for you, but they would not be able to view your profile/photographs or comments until they are listed as a friend in your contacts list.

6.2 Search
You are able to change a setting within the privacy tab to stop people from finding your profile when they perform a search. The Facebook search facility makes it easy for anyone to enter your first name and/or surname into the search field and find a list of all the users on the site matching that name. Users are then able to sort within the results to narrow down the list of names more specifically by using other sorting options e.g. by locations, age, status, gender, location and many more. The following settings can be changed in relation to searching:

Allow anyone to see my public search listing
If you want people you know to know that you are on Facebook, leave this unselected.

Allow my public search listing to be indexed by external search engine
If set to "yes", your details will be available via search engines such as Google and MSN.
If you allow others to search for your profile within Facebook, they will be able to do the following:

- See your profile pictures
- Send you a message
- Add you as a friend
- View your friend list

If you haven't restricted your profile settings (see Section 6.1 above), the person who performed the search can view your profile fully.

6.3 Poke Messages and Friend Requests
Sending a poke, replying to a message or receiving a friend request temporarily allows that user to view your profile even if your normal privacy settings would not allow them to do so. This area allows you to control what profile information you wished to be visible. You should also be careful about who you reply to, if in any doubt you could block a user.

6.4 Block People
An option is available to block another user. They will not be able to search for you, view your profile or contact you on Facebook. Any current connections you have with that user will be removed (e.g. friendship, relationship). You can use this if you are having problems with a particular person trying to contact you.

7. Application Settings
Applications within Facebook include additional "add on" functionality, so for example, interest groups, games, events, videos etc. You can edit the settings to allow or restrict the view of which applications you have added to your profile. You can customise this to allow selected friends to see which applications you have added but not all. The following options are available to choose from:

- Everyone
- My network and friends
- Friends of friends
- Only friends
- Only me
- Customise

Personal use of Social Media Sites

I have read, understood and agree to abide by this policy. I understand that employees and governors of ACADEMY NAME are expected to adhere to the policy and procedure and ensure that they conduct themselves in a manner that will not place children or vulnerable adults at risk, bring ACADEMY NAME into disrepute or damage their own professional reputation.

Name:

Signature:

Date: