Contents

Introduction

This policy covers personal use of social media as well as for official school purposes including sites hosted and maintained on behalf of the School. It applies to the use of social media during working hours or otherwise and whether the social media is accessed using the School's IT facilities, equipment belonging to members of staff or any other IT resource.

This document applies to all staff who work in the school whether paid or unpaid. The term 'staff' applies to all employees of the school, Governors, volunteers, contractors and Chartwells employees. This policy does not form part of your contract of employment and it may be amended at any time.

All staff working within the school setting are accountable for information published and must be aware that such information may be monitored by the Headmaster or the Marketing department. It is important to note that information available in the public domain which has the potential for harm, distress or reputational damage may lead to disciplinary action being taken.

What Social Media activity does this policy cover?

This policy is mainly concerned about two types of social media activity:

- Your own personal activity, not under or in the name of St Faith's school.
- Activity carried out in the name of St Faith's school, such as a school Facebook or Twitter post that represents, or appears to represent, the official views of the school.

This policy aims to ensure that your use of social media does not harm the interests of the children we support, or damage the reputation of the school or school staff. Adherence with the good practice

guidelines in this document will help protect you against posting things that you might regret or may harm you later.

This policy and guidance will help to make sure that your use of social networking sites and social media is safe.

The Policy

Social Networking "Must Nots":

- You must not make comment on behalf of the school or claim to represent the views of the school, unless you have explicit permission to do so.
- Never use personal devices for social media posts which include photographs of pupils.
- Never make a 'friend' of a pupil at the school when you are on your social networking page and seek the advice of the Headmaster or Deputy Head before becoming 'friends' with ex-pupils.
- Exercise caution when making 'friends' with a parent/carer of a pupil at the school.
- Never use or access social networking pages of pupils.
- Do not request, or respond to, any personal information from a pupil.
- Never post confidential information about yourself, the school, the Governing body, your colleagues, pupils or other individuals connected with the school or another school. If you have concerns about practices within the school or the actions of pupils or parents you must act in accordance with the school's Whistleblowing policy.
- Never use social media for personal use during working hours by means of the school's IT resources and communication systems.
- Do not post images of yourselves or pupils wearing clothing with identifiable school crests on, or any images that directly relate to the school in anyway, unless using the school's official Facebook or Twitter accounts for purposes pre-agreed with the Headmaster or Marketing Department. If you are a staff member and also a parent you must exercise extreme caution when posting images of your own children in school attire on your social media feeds, and you should specifically consider all the guidelines mentioned herewith.

Social Networking "Shoulds":

You should regularly review your social networking sites to ensure that information available publicly about you is accurate and appropriate. This includes any photographs that may cause embarrassment to you and/or the school if they were to be published outside of the site.

- Be aware of the dangers of putting your personal information onto social networking sites such as addresses, home or mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to you outside the school environment. It also reduces the potential for identity theft by third parties.
- Ensure your privacy settings are appropriately set on any personal social media accounts you use. This will ensure that you are only followed by people you know and have granted permission to view your account and will prevent your information being used inappropriately.
- Be aware that some social networking sites and other web-based sites have fields in the user profile for job title etc. As an employee or volunteer of the school and particularly if you are a teacher or teaching assistant, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school and the profession. If it is a work-based site where you are required to provide this information, you must obtain the permission of the Headmaster or Deputy Head beforehand, unless the site is on the list of approved sites for the school. *The one exception to this rule is the listing of St Faith's as your current employer on LinkedIn and is to be used purely for the purposes of professional development. Staff with*

LinkedIn accounts which reference their employer as St Faith's should notify the Marketing Manager that they have such an account for the purposes of record keeping.

- When Tweeting from a school account you should consider the general ethos as 'observing facts, rather than stating opinions.'
- You may only use images of pupils where the school has been permitted to use their images in digital communications. A current list of those not giving photographic permissions is on the VLE, Staff Area, Marketing Page. Remember: never use personal devices for Tweets which include photographs of pupils.
- When Tweeting from a school account seek permission from the relevant public figures or organisations before citing their work in relation to any school activity.
- Report to the Headmaster or Marketing department immediately if you see any information on the internet or on social networking sites that disparages or reflects poorly on the school.

Social Networking Good Practice

You must understand who is allowed to view the content of your pages on any sites you use and how to restrict access to certain groups of people.

- On Facebook, you should understand whether the posts you make are Public (which means that anyone can see them), visible to Friends (which means that only people on your Friends list can see them) or visible to Friends of Friends, which means that the posts are visible to all the friends of your friends, which could be many hundreds or even thousands of people.
- On Twitter and LinkedIn, all posts, unless they are direct messages to another user, are visible to everyone (worldwide).
- On Instagram, all posts are visible publicly unless you create a 'private' account.
- If you are unsure of who can see your posts on other sites, you should always assume that the information is publicly available to all and could be found by people doing a search on Google, for example.
- It is recommended that all your social media profiles are set to 'private'.

Before posting, you should ask yourself the following questions:

1. Do you want the whole world to see? Even if you restrict your own visibility settings, these can be overridden by the settings of others, or people can copy and paste the information into other public places.
2. Do you want the post to be seen forever? Once you have posted something, it is almost impossible to delete it again from the internet, even if you delete it from the site. There are sites that archive all Twitter posts, for example, so even if you delete a post from Twitter, it can still be found.
3. What if the information is taken out of context? It is very easy for others to take what is posted, alter it, and re-post it elsewhere. It is also possible that your hard work, posted online, may be used inappropriately by others.
4. Are you violating any laws? The information could breach copyright, or specific legislation relating to privacy of vulnerable groups, for example. What you post could be illegal in other countries, which could have serious implications if you were to later visit there. Are you making claims that could be taken as facts when they are not? This could lead to you being accused of slander.
5. If music is part of your post please ensure that sharing the post will not infringe any copyright on the music as this may result in the post being removed and in extreme cases legal action against the school.
6. Is your message clear? Could you unintentionally be breaking cultural norms or putting out something unintentionally offensive. Is it clear whether or not you are posting in an official capacity?

7. Could the actions of your social networking friends reflect on you? Could your friends or friends of friends 'tag' you in photographs or link you to inappropriate activities through their own posts? Choose your friends carefully.

If you have any doubts you should seek advice from the Headmaster or Head of Marketing and Admissions.

Posting on behalf of the school

You are not permitted to post on behalf of the school without specific permission, which will apply to specific sites (only Twitter and Facebook applicable presently). For example, the Headmaster or Marketing Manager may give permission for you to post as teachers at St Faith's school when reporting on sports fixtures, day or residential trips. In such cases the Headmaster or Marketing Manager will make clear the capacity in which you may post and the scope and subject of your postings. The Marketing Manager will keep a central log of all those who may post on behalf of or as a representative of the school. Remember, you must not use your personal devices to take photos for sharing via the school Twitter or Facebook pages.

When posting on behalf of the school it is imperative that even in the heat of the moment, i.e. on the touch-line of a sports fixture, that great attention is paid to accurate spelling, grammar and punctuation as any Tweet or Facebook post is a reflection on the school and the quality of the education we provide.

Breaches of the policy

Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and whether the school's equipment or facilities are used for the purpose of committing the breach. Any members of staff suspected of committing a breach of this policy will be required to cooperate with an investigation, which may involve handing over relevant passwords and login details so far as this is consistent with the rights of an individual to private and family life. You may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Implementation of the policy

The Headmaster has overall responsibility for the effective operation and reviewing of this policy. Responsibility for monitoring the operation of this policy and making recommendations for change to minimise risk lies with the Marketing Manager. All heads of department and senior managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and, if necessary, enforcing this policy by taking action when behaviour falls below its requirements.

Monitoring

The contents of the School's IT resources and communications systems are the school's property. Therefore, you should have no expectation of privacy in any message, file, data, document, facsimile, telephone conversation, social media post, message, or any other kind of information or communications stored on, transmitted to or received from the School's electronic information and communications systems. The School reserves the right to monitor, intercept and review, without further notice, staff activities using IT resources and communications systems including, but not limited to, social media postings, to ensure that the policy is being complied with and for legitimate business purposes. Your consent to such monitoring is given by your use of such resources and systems. The school may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

If you become aware of any inappropriate use of social media by a colleague please contact the Headmaster or Head of Marketing immediately or refer to the procedures outlined in the School's Whistleblowing Policy.

End of employment

When your employment with the school ends, for whatever reason, if consent has previously been given for any personal profiles on social networking sites to identify the link between the School and you, such profiles should be immediately amended to reflect the fact that you are no longer employed or associated with the school.

Additional Information:

Legal Framework

St Faith's is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the School 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, the Data Protection Act 1998 and St Faith's Network Agreement.

Confidential information includes, but is not limited to: person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 1998; 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; politically sensitive information.

Staff 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; Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services, 2008; Communications Act 2003; Copyright, Designs and Patents Act 1988.

St Faith's could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of any protected characteristic including race, sex, disability, etc. or who defame a third party in a manner connected to their employment may render St Faith's liable to the injured party.

Cyberbullying

Cyberbullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'
If cyberbullying does take place, you should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. You are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site. You are encouraged to report any and all incidents of cyberbullying to your line manager or the Headmaster. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police. If you become aware of a pupil being subject to cyberbullying, you should raise it with your line manager or Headmaster.