

## Forres Sandle Manor (Non-Academic) Policy

Policy Title	<b>Social Media</b>
Policy Lead (Appointment (& Initials))	<b>Head of Marketing and Admissions (SSi)</b>
Date of Last Review	<b>September 2018 (mid term review January 2020)</b>
Date of Next Review	<b>September 2020</b>

### SOCIAL MEDIA

#### **INTRODUCTION**

The school is aware and acknowledges that increasing numbers of adults and children are using social networking sites. The widespread availability and use of social networking applications bring new opportunities to understand, engage and communicate with audiences in new ways. It is important that we can use these technologies and services effectively and flexibly. While recognising the benefits of these media, this policy sets out the principles that Forres Sandle Manor School (FSM) staff and contractors are expected to follow when using social media.

It is crucial that pupils, parents and the public at large have confidence in FSM's decisions and services. The principles set out in this policy are designed to protect staff, to ensure that staff members use social media responsibly so that confidentiality of pupils and other staff and the reputation of FSM are safeguarded and advise school leadership on how to deal with potential inappropriate use of social networking sites.

Staff members must be conscious always of the need to keep their personal and professional lives separate.

#### **SCOPE**

This policy applies to FSM School governing body, all teaching and other staff, external contractors providing services on behalf of the school, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to as 'staff members' in this policy.

This policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school.

This policy applies to personal webspace such as social networking sites (for example *Facebook*, blogs, microblogs such as *Twitter*, *Instagram*, *Spotify*, chatrooms, forums, podcasts, open access online encyclopaedias such as *Wikipedia*, social bookmarking sites such as *Del.icio.us*, *Pinterest* and content sharing sites such as *flickr*, *YouTube* and

*musical.ly*. 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.

## **LEGAL FRAMEWORK**

FSM 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.
- General Data Protection Regulation 2018

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 1998 and GDPR 2018.
- 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 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.
- Copyright, Designs and Patents Act 1988.

FSM School 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 FSM School liable to the injured party.

## **RELATED POLICIES**

This policy should be read in conjunction with the following school policies:

- Data Protection Policy. (incl GDPR)
- Password Policy.
- Safeguarding Policy.
- Behaviour and Disciplinary Policy.
- Staff Code of Conduct.
- E-Safety Policy.
- Staff Handbook.
- Acceptable Use Policy and Children's User Agreement.

### **PRINCIPLES – *BE PROFESSIONAL, RESPONSIBLE AND RESPECTFUL***

- You must be conscious always of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the school and your personal interests.
- You must not engage in activities involving social media which might bring FSM School or its employees, pupils, parents, governors, contractors or suppliers into disrepute, for example by posting images or video clips that are inappropriate or links to inappropriate website content.
- You must not represent your personal views as those of FSM on any social medium.
- You must not discuss personal information about pupils, FSM staff and other professionals you interact with as part of your job on social media.
- You must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations or FSM.
- You must be accurate, fair and transparent when creating or altering online sources of information on behalf of FSM.
- You must not breach copyright or any other proprietary interest belonging to FSM, for example, using someone else's images or written content without permission or failing to give acknowledgement where permission has been given to reproduce particular work.

Employees must remove any offending content immediately if they are asked to do so by the School.

Should employees notice any inaccurate information about FSM online, they should report this to the Marketing Manager and Head.

### **PERSONAL USE OF SOCIAL MEDIA**

FSM recognises that many employees make use of social media in a personal capacity outside the workplace and outside working hours. While they are not acting on behalf of the School in these circumstances, employees must be aware that they can still cause damage to the School if they are recognised online as being one of its employees. Therefore, it is important that the School has strict social media rules in place to protect its position.

- Staff members should not identify themselves as members of FSM in their personal web-space unless specifically linked to an approved job role within the School community where it serves a purpose to professionally market the school. This is to prevent information being linked with the school and to safeguard the privacy of staff members, pupils, parents and the wider school community.
- Staff members must not have contact through any personal social medium with any pupil, whether from FSM or any other school, unless the pupils are family members.
- Staff may not be friends with any ex-student until they reach the age of 21. FSM School does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain during their employment must not be used for personal gain nor be passed on to others who may use it in such a way.
- 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.
- Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy.
- Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information.
- It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

### **Guidance/protection for Pupils on using social networking**

No pupil under 13 should be accessing social networking sites.

There is a mechanism on many social media sites where pupils can be reported, usually via the Help screen or button. For example, under age Facebook user can be reported using the following link: [http://www.facebook.com/help/contact.php?show\\_form=underage](http://www.facebook.com/help/contact.php?show_form=underage)

### **Child Protection Guidance**

If any member of staff receives a disclosure that an adult employed by the school is using a social networking site in an inappropriate manner as detailed above, they should:

- Record the disclosure in line with the Child Protection Policy.
- The Head will refer the matter to the Local Authority Designated Officer (LADO) who will investigate via the Hampshire Safeguarding Children Board.
- If the disclosure has come from a parent, pass the information on to the Designated Safeguarding Lead (DSL), who in this school is the Deputy Head, Mr Jody Wells, immediately.
- If the disclosure comes from a member of staff, pass the information on to the Head immediately. The LADO will advise whether the member of staff should be

suspended pending investigation after contact with the police. It is not recommended that action is taken until advice has been given.

- If the disclosure is from a child, follow our normal processes as instructed in our child protection policy until the police investigation has been carried out.

## **MONITORING OF INTERNET USE**

FSM School monitors usage of its internet and email services without prior notification or authorisation from users. *See e-Safety Policy*

## **BREACHES OF THE POLICY**

Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with FSM School Disciplinary Policy and Procedure.

A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of FSM School or any illegal acts or acts that render FSM School liable to third parties may result in disciplinary action or dismissal.

**Contracted providers of FSM School services must inform the FSM Marketing Manager immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school. Any action against breaches should be according to contractors' internal disciplinary procedures.**

**Any other safeguarding concerns should be raised with the DSL.**

## **Annex 1: Requirements for creating social media sites on behalf of FSM**

### **CHILDREN AND YOUNG PEOPLE**

- When creating social media sites for children and communicating with them using such sites, staff members must always be conscious of their responsibilities; staff must always act in the best interests of the children.
- When creating sites for children, staff members must be alert to the risks to which young people can be exposed. Young people's technical knowledge may far exceed their social skills and awareness – they may post sensitive personal information about themselves, treat online 'friends' as real friends, be targets for 'grooming' or become victims of cyberbullying.
- Sites and material created for children must be set to private so that it is not searchable online.
- If children disclose information or display behaviour or are exposed to information or behaviour on these sites that raises safeguarding or other concerns, appropriate authorities must be informed immediately. Failure to do so could expose vulnerable young people to risk of harm.
- Staff members must ensure that the sites they create or contribute to for work purposes conform to the *Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services* (Home Office Task Force on Child Protection on the Internet, 2008).
- Staff members must also ensure that the webspace they create on third party sites comply with the site owner's minimum age requirements (this is often set at 13 years). Staff members must also consider the ramifications and possibilities of children under the minimum age gaining access to the site.
- Care must be taken to ensure that content is suitable for the target age group and contributors or 'friends' to the site are vetted.
- Careful thought must be given to the profile of young people when considering creating sites for them. For example, the internet may not be the best medium to communicate with vulnerable young people (or indeed any age group) receiving confidential and sensitive services from the school. It may not be possible to maintain confidentiality, particularly on third-party-hosted sites such as social networking sites, where privacy settings may not be strong enough to prevent breaches of confidentiality, however inadvertent. If in doubt, you must seek advice from your Network Manager.

### **APPROVAL FOR CREATION OF OR PARTICIPATION IN WEBSPACE**

The Marketing Team have full responsibility for running the school's official website, Facebook, Twitter, Instagram, SoundCloud, Wordpress, Issuu and YouTube sites. No other social media platforms may be set up by any member of the whole school community which have a direct or indirect connection with FSM.

- FSM School social media sites can be created only by or on behalf of the school.
- Site administrators and moderators must be FSM School employees or other authorised people.

- Approval for creation of sites for work purposes, whether hosted by the school or hosted by a third party such as a social networking site, must be obtained from the staff member's line manager, FSM's Marketing Manager and Head.
- Approval for participating, on behalf of FSM School, on sites created by third parties must be obtained from the staff member's line manager, the FSM's Marketing Manager and Head.
- Content contributed to own or third-party hosted sites must be discussed with and approved by the staff member's line manager and the Marketing Manager.
- FSM's Marketing Manager must be consulted about the purpose of the proposed site and its content. In addition, the Marketing Manager's approval must be obtained for the use of the school logo and brand.
- Be aware that the content or site may attract media attention. All media enquiries must be forwarded to the Marketing Manager and Head immediately.
- Staff members, must not communicate with the media without the advice or approval of the Head.

### **CONTENT OF WEBSITE**

- FSM School -hosted sites must have clearly expressed and publicised Terms of Use and House Rules. Third-party hosted sites used for work purposes must have Terms of Use and House Rules that conform to the school of professional conduct and service.
- Staff members must not disclose information, make commitments or engage in activities on behalf of FSM School without authorisation.
- Information provided must be worthwhile and accurate; remember what is published on the site will reflect on the school's image, reputation and services.
- Stay within the law and be aware that child protection, privacy, data protection, GDPR, libel, defamation, harassment and copyright law may apply to the content of social media.
- Staff members must respect their audience and be sensitive in the tone of language used and when discussing topics that others may find controversial or objectionable.
- Permission must be sought from the relevant people before citing or referencing their work or referencing service providers, partners or other agencies.
- FSM School -hosted sites must always include the school logo or brand to ensure transparency and confidence in the site. The logo should, where possible, link back to the relevant page on the school website.
- Staff members participating in FSM School hosted or other approved sites must identify who they are. They must disclose their positions within the school on these sites.
- Staff members must never give out their personal information such as home contact details or home email addresses on these sites.
- Personal opinions should not be expressed on official sites.

## **CONTRIBUTORS AND MODERATION OF CONTENT**

- Careful consideration must be given to the level of engagement of contributors – for example whether users will be able to add their own text or comments or upload images.
- Sites created for and contributed to by pupils must have the strongest privacy settings to prevent breaches of confidentiality. Pupils and other participants in sites must not be able to be identified.
- The content and postings in FSM School -hosted sites must be moderated. Moderation is the responsibility of the team that sets up or initiates the site.
- The Network team must designate at least one member of staff whose role it is to review and moderate the content in contact with the marketing team, including not posting or removal of comments which breach the Terms of Use. It is important that there are enough approved moderators to provide cover during leave and absences so that the site continues to be moderated.
- For third-party-hosted sites such as social networking sites used for work purposes, the responsibility for protection and intervention lies first with the host site itself. However, different sites may have different models of intervention and it is ultimately the responsibility of the staff member creating the site to plan for and implement additional intervention, for example in the case of content raising child safeguarding concerns or comments likely to cause offence.
- Behaviour likely to cause extreme offence, for example racist or homophobic insults, or likely to put a young person or adult at risk of harm must never be tolerated. Such comments must never be posted or removed immediately and appropriate authorities, for example the Police or Child Exploitation and Online Protection Centre (CEOP), informed in the case of illegal content or behaviour.
- Any proposal to use social media to advertise for contributors to sites must be approved by the FSM's Marketing Manager.
- Approval must also be obtained from the Marketing Manager (to make an external organisation a 'friend' of the site).