FALINGE PARK HIGH SCHOOL

SOCIAL MEDIA POLICY

Date: June 2018

Falinge Park High School Social Media Policy

Document Control

Organisation	Falinge Park High School
Title	Social Media Policy
Author	IT Strategy Group
Filename	FPHS Social Media Policy 2015
Owner	IT Strategy Group
Subject	Social Media
Review date	01/07/2017

Revision History:

Revision Date	Reviser	Previous Version	Description of Revision
01/07/2016	ICT STRAT	01/07/2015	No revisions made
01/07/2017	ICT STRAT	01/07/2015	No revisions made
08/07/2018	SWA	01/07/2015	updates in line with e-Safety and AUP policy updates

Document Approvals – This document requires the following approvals:

Approval Sought From	Name	Date
Governors	Resources Committee	Draft Summer 2015 Adopted
Governors	Pupil and Curriculum	Adopted
Governors	Pupil and Curriculum	September 2018

Document Distribution – This document will be distributed to:

Individual/Group	Job Title/Group Type	Distribution Date
All Staff	All Job Titles	04/09/2015
All Staff	All Job Titles	September 2018

Introduction

This policy should be read in conjunction with other relevant policies e.g. e-Safety and Acceptable Use Policy, Data Protection Policy, Information and Systems Security Policy, Disciplinary Policy and Procedures, Equal Opportunities Policy, Codes of Conduct.

All school employees or volunteers need to be aware of the risks and accountability of inappropriate or inadvertent provision of information about themselves, the school or its pupils and staff or the wider school community in the Social Media arena.

All school employees or volunteers working within the school setting are accountable for information published and must be aware that such information may be monitored by the e-Safety co-ordinator (Mr S Ward) and the ICT technical team.

It is important to note that information available in the public domain which has the potential for harm, distress or reputational damage to the school, staff or pupils may lead to disciplinary action being taken by the school.

What is Social Networking and Social Media?

- Social networking and social media are communication tools based on websites or networks which allow users to share information or other material about themselves and their interests with groups of other people.

These groups of people could be:

- People who are known to you (friends or colleagues)
- People you don't know but who share common interests (such as Teaching, working in Rochdale, etc)
- Anyone who could find your comments through search engines.

Examples of Social Media and Social Networking sites and services include:

- Facebook
- Snapchat
- Instagram
- Pinterest
- Twitter
- YouTube
- LinkedIn
- Blogs
- discussion groups
- mailing lists

What social media activity does this policy cover?

This policy is mainly concerned about two types of Social Media activity:

- Your own **personal activity**, done for your friends and contacts, but not under or in the name of Falinge Park High School (or Rochdale Borough Council), however could include comments related to or involving Falinge Park High School, its staff or students.
- Activity carried out in the name of **Falinge Park High School**, such as a school blog or Twitter posting or a Facebook Group that represents, or appears to represent, the official views of the school.

This policy is not about stopping you using or accessing such groups, but aims to ensure that your use of social media does not harm the interests or damage the reputation of any member of our school community. Adherence with the good practice guidelines in this document will help protect you against posting things that you might regret or that might cause damage to your professional reputation and future career prospects.

Aim of this policy

This policy recognises that new technologies are an integral and growing part of everyday life and make an important contribution to teaching and learning opportunities. However the rapid evolution of social networking technologies requires a robust policy framework and this policy aims to:

- Assist all school employees or volunteers working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary and/or legal action will be taken
- Support safer working practice
- Minimise the risk of misplaced or malicious allegations made against any school employees or volunteers who work with pupils
- Prevent any school employees or volunteers abusing or misusing their position of trust.

This document applies to **all staff** who work in the school whether paid or unpaid. This includes members of the Governing Body, whether Parent, Community or Local Authority Governors.

Principles

The principles that underpin this policy are:

- All school employees or volunteers who work with pupils are responsible for their own actions and behaviour and must avoid any conduct which would lead any reasonable person to question their motivation and intentions.
- All school employees or volunteers in the school must work and be seen to work, in an open and transparent way.
- All school employees or volunteers in the school must continually monitor and review their own practice in terms of the continually evolving world of social networking and ensure that they consistently follow the guidance contained in this document.

Why do we need the policy?

There have been numerous examples of people in all walks of life posting things in social media that they have later regretted, because that information has harmed or put at risk themselves or others. This includes:

- Accidentally posting personal or embarrassing information about themselves or others in a public forum or beyond the group the information was originally intended for.
- Sharing information about yourself or others with people you don't know that could be used by someone to commit fraud or misrepresent the views of yourself or others (such as identity theft)
- Breaching privacy or child protection laws and regulations or workplace policies by posting information about your work or the children and adults that you work with
- You or others receiving negative publicity, harassment, inappropriate contact or threats as a result of your views, beliefs or comments.
- staff being unaware of pupils following them through indirect contacts via social media accounts
- staff believing that they are “locked down” in terms of their social media profile privacy settings when they have left themselves vulnerable through accepting family members or ex students which subsequently grants access to other users on the social media network

This has led to people facing disciplinary action, losing their jobs and being prosecuted.

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

Safer Social Networking Practice

This document applies to current social networking sites such as Snapchat, Facebook, Youtube, Instagram, Twitter etc and all other current and emerging technologies.

The Safer Social Networking Practice is broken down into:

- Things you must not do, because they are illegal, contrary to regulations or against school policy (such as professional boundaries)
- Things you should do to avoid risk to yourself or others
- Good Practice suggestions to reduce the risk of your personal information being misused

All school employees or volunteers must adhere to, and apply the principles of this document in all aspects of their work. Failure to do so may lead to action being taken under the disciplinary procedure.

Social Networking “Must Nots”

All school employees or volunteers:

- must not make any negative or confidential comments on behalf of the school unless they have explicit permission to do so from either the Headteacher or e-Safety coordinator (Mr S Ward). Nor should they claim to represent the views of the school or any other member of the school community (eg. governing body, PTA) or the LA.
- should never make a ‘friend’ of a pupil at the school where they are working on their personal social networking page. Ex-students must not be added within the L.A. recommended 5 year period. Special care should be taken when accepting ex-students at any stage as they may have friends or siblings who are currently at the school who will then have access via their profiles.
- should not make a “friend” of a parent/carer of a pupil at the school. The only exception to this is where staff are personal friends or colleagues.
- should never use or access social networking pages of pupils except in the case of technical staff who may be investigating an e-Safety/bullying issue where this has been referred to them by the e-Safety coordinator (Mr S Ward). In addition, technical staff must ensure there is another member of staff present when undertaking investigations.
- must not request, or respond to, any communication or requests made via personal social media from a pupil (past or present) outside of established

school communication systems. Refer to the e-Safety and Acceptable Use Policy for clarification. Requests of this nature must be immediately reported to the e-Safety coordinator (Mr S Ward).

- not put any information onto personal social networking sites that could identify either your profession or the school where you work. This is often collected by these sites during the process of setting up an account profile. In negative circumstances this could damage the reputation of the school.
- Access or use social media accounts through the school systems or personal devices during the period of the working day.

Social Networking "Shoulds"

All school employees or volunteers (particularly those new to the school setting) should:

- review their privacy settings on social networking sites (and those of friends/family where their info may be shared) on an ongoing basis to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and/or the school.
- review their current "friends" to ensure that they do not contravene any of the statements in the "should not" section. This is particularly important for new staff who may enter the school with previous friendships that could contravene the expectations set out by this policy.
- be aware of the dangers of putting their personal information onto social networking sites such as **addresses, home or mobile phone numbers**. This will avoid the potential for personal contact by pupils or their families or friends. It also reduces the potential for identity theft by third parties.
- for work-based social networks (where you are required to provide profile information) eg. exam board forums, etc, you must ensure any shared information will not be in breach of the school e-Safety and Acceptable Use Policy or Data Protection Policy. All information that is to be posted on the schools social media accounts must be sent to the e-Safety coordinator (Mr S Ward) for approval prior to posting.
- keep their personal phone numbers, work login, passwords and personal email addresses private and secure. Where there is a need to contact pupils or parents the school email system and/or telephone should be used. If, with permission, telephone calls are made from a personal phone (landline or mobile phone) the telephone number the call is being made from must be withheld by prefixing the dialled number with 141.
- ensure that all communications undertaken **via approved school social media accounts** are positive, transparent and open to scrutiny. They should also be circumspect in order to avoid any possible misinterpretation of their

motives or any behaviour which could possibly be construed as ‘grooming’ in the context of sexual offending.

- communications between a member or staff or volunteer and a pupil should only take place within agreed school systems (eg. SchoolComms or approved FPHS@addresses within social media) and all within the confines of the e-Safety and School Acceptable Use Policy.

Social Networking Good Practice

All school employees or volunteers must understand who is allowed to view the content on their pages of any sites they use and how to restrict access to certain groups of people.

- On Facebook, they should understand whether the posts they make are Public (which means that anyone can see them), visible to Friends (which means that only people on their Friends list can see them) or visible to Friends of Friends, which means that the posts are visible to all the friends of their 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 (the whole world)
- Due to the mass use of Snapchat by the pupils currently at the school it is further highlighted to staff the importance of protecting themselves through the administration of the guidance within this policy during their use of this social media platform to ensure that contact with students is avoided.
- 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.

For support with any of these good practices, please contact the ICT technician and they will work with you to ensure that you social media is safe.

Before posting, all school employees or volunteers should ask themselves 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, is it 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. Could the information put you or others in danger? What you post could tell others that your house is empty or that the pupils in your class are on a school trip, which could have implications for a looked-after child.
5. 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 that could be taken as facts when they are not? This could lead you to being accused of slander.
6. Is your message clear? Could you be unintentionally 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 or friends "tag" you in photographs or link you to inappropriate activities through their own posts? Choose your friends and discuss your preferred settings with them carefully.

If you have any doubts about any other these, you should seek the advice of the e-Safety Coordinator – Mr S Ward or the Head Teacher.

- If staff are uncertain or are concerned about any personal interaction with pupils past and present or parents via any of their 'personal' social media accounts, they should refer this in the first instance to the e-Safety coordinator, and take immediate action to protect their information.

- If staff wish to seek further advice about how to protect their personal information held within 'personal' social media accounts they should speak to the school IT technical team or the school e-Safety Coordinator.

It is your personal and professional responsibility to ensure that you are safe and acting in accordance to the professional standards set out in this and other policies. Breaking these expectations may result in disciplinary actions being taken by the school.