Social Media

Lead Reviewer: **Man Wong**

Who this is aimed at: **The whole school community**

Version	Reason for Change
1	
2	Governors' review added updates: Page 2: data protection changed to refer to GDPR Example re family relationships added Safer recruitment – add social media to recruitment checklist conversation Frequency of review: biannually

Frequency of review	2 years	**Review due**	March 2021

This policy will cover any media that is put in the public domain.

This policy should be read with reference to the following policies:

- GDPR statement
- ICT and E-Safety by staff policy
- Child protection and Safeguarding policy
- Disciplinary policy
- Grievance policy

Rosewood free School finds itself in a unique position when considering the use of social media. We are a school for children and young people with complex medical, health and social needs. Families rely on us as a source of support and advice in ways that are outside of the normal family and school relationship. In a modern world where social media is key to daily communication of most people we must, if we are going to meet our family's needs, take account of this.

In addition to this we employ several parents within the school and respect that friendships between staff and parents may develop in this situation. Pre-existing friendships between staff and families (for example a new staff member joining the team because the know a child or family currently at the school) are to be declared to the senior leadership team to enable appropriate boundaries to be established within the professional relationships that may include not teaching that child or young person or having direct responsibility for meeting their needs.
As part of our Safer Recruitment practice we have a conversation about social media at every interview for a new member of staff.

Sometimes the only way we can have communication with our hard to reach families is through the use of social media. This policy is written to reflect this and endeavours to protect our staff whilst acknowledging that for the deputy head and head teacher, social media may and will be used to provide meaningful contact for families. This will be done as transparently as possible and through the use of school mobile devices.

Definition of social media

For the purposes of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes e-mail, online social forums, blogs, video- and image-sharing websites and similar facilities.

Employees should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area. Employees should follow this policy in relation to any social media that they use.

This policy aims to:

- Assist those who work with pupils to work safely and responsibly, to monitor their own standards of behaviour and to prevent the abuse of their position of trust with pupils.
- Offer a code of practice relevant to social media for educational, personal and recreational use.
- Advise that, in the event of unsafe and/or unacceptable behaviour, disciplinary or legal action (including gross misconduct leading to dismissal) will be taken if necessary in order to support safer working practice and minimise the risk of malicious allegations against staff and others who have contact with pupils.

While acknowledging the benefits of social media and the internet it is also important to recognise that risk to the safety and well-being of users is ever-changing and that the misuse/abuse of these facilities can range from inappropriate to criminal and schools need to have mechanisms in place to deal with misuse of social media. Misuse can be summarised in the following list that is a guide only and does not cover all aspects of misuse due to the wide and varied nature of the use of social media and the speed at which it changes:

Contact

- Commercial (tracking, harvesting personal information).
- Aggressive (being bullied, harassed or stalked).
- Sexual (meeting strangers, being groomed).
- Values (self-harm, unwelcome persuasions).

Conduct

- Commercial (illegal downloading, hacking, gambling, financial scams).
- Aggressive (bullying or harassing another).
- Sexual (creating and uploading inappropriate material).
- Values (providing misleading info or advice).

Content

- Commercial (adverts, spam, sponsorship, personal information).
- Aggressive (violent/hateful content).
- Sexual (pornographic or unwelcome sexual content).
- Values (bias, racism, misleading info or advice).

Use of social media within school
Staff are not permitted to access social media websites from the school's computers or other school devices at any time unless authorised to do so by a member of the senior leadership team. However, staff may use their own devices to access social media websites while they are in school, outside of session times, during breaks and lunch, before and after school.

Staff should assume that anything they write (regardless of their privacy settings) could become public so should ensure that they are professional, maintaining a clear distinction between their personal and professional lives.

Any use of social media of any form made in any capacity must not:

- Bring the school into disrepute.
- Breach confidentiality.
- Breach copyrights of any kind.
- Bully, harass or be discriminatory in any way.
- Be defamatory or derogatory.

Use of social media outside of school
The school appreciates that staff may make use of social media in a personal capacity. However, staff must be aware that if they are recognised from their profile as being associated with the school, opinions they express could be considered to reflect the school's opinions and so could damage the reputation of the school. For this reason, staff should avoid mentioning the school by name, or any member of staff by name or position. Opinions offered should not to bring the school into disrepute, breach confidentiality or copyright, or bully, harass or discriminate in any way.

General considerations
Those working with children have a duty of care and a statutory duty to report signs of potential radicalisation but also need to be on the lookout for cyber bullying and other activities on social media which might affect the mental health of pupils.

Staff need to be aware that those attempting to groom youngsters for radicalisation are known to work through social media such as: Facebook, Twitter, YouTube, Ask.fm, Instagram, Tumblr and closed peer-to-peer networks such as WhatsApp, Kik, SureSpot and Viber.

When using social media staff should:

- Never share work login details or passwords.
- All email communication between staff and members of the school community on school business must be made from an official school email account, personal emails should not be shared.
- Keep personal phone numbers private, a school mobile is available for use and the head teacher and deputy head teacher have work mobile numbers that can be shared with families and staff members that are used for communication outside of school working hours. This is essential when considering the nature of the school population and the need for urgent contact in some situations.
- The school has the use of Teachers to Parents from which individual texts can be sent to families if necessary, by the admin team or head teacher and deputy head teacher.
- Restrict access on their social media sites and pages.
- Not make 'friends' of pupils at the school because this could potentially be construed as 'grooming', nor should they accept invitations to become a 'friend' of any pupils past or present.
- Carefully consider contact with a pupil's family members because this may give rise to concerns over objectivity and/or impartiality. In the event of this being deemed as necessary to promote the welfare and safety of a child or young person this must be shared with the senior leadership team to maintain transparency and to legitimise this communication.
- Staff should only use the school's systems for communications. (If there is any doubt about whether communication between a pupil/parent and member of staff is acceptable and appropriate a member of the senior leadership team should be informed so that they can decide how to deal with the situation).
- Any communication received from children on any personal social media sites must be reported to the designated safeguarding lead. Members of the school staff are strongly advised to set all privacy settings to the highest levels on all personal social media accounts (support is available with how to do this).

Before joining the school, new employees should check any information they have posted on social media sites and remove any post that could cause embarrassment or offence.

Disciplinary action
Any breach of this policy may lead to disciplinary action under the school's disciplinary policy. Serious breaches of this policy, such as incidents of bullying or of social media activity causing damage to the organisation, may constitute gross misconduct and lead to dismissal.

Staff must be aware of what is considered to be 'criminal' when using social media or the internet and electronic communication in general.

While the list below is not exhaustive, it is provides some guidance in assessing the seriousness of incidents as well as determining appropriate actions.

All incident types below are considered criminal in nature but incidents would be subject to a full investigation in order to determine whether a crime has been committed or not. Staff must be aware that downloading multimedia (music and films) on premises that has copyright attached is an offence.

- Copyright infringement through copying diagrams, texts and photos without acknowledging the source.
- Misuse of logins (using someone else's login).
- Distributing, printing or viewing information on the following:
- Soft-core pornography.
- Hate material.
- Drugs.
- Weapons.
- Violence.
- Racism.
- Distributing viruses.
- Hacking sites.
- Gambling.
- Accessing age restricted material.
- Bullying of anyone.
- Viewing, production, distribution and possession of indecent images of children.
- Grooming and harassment of a child or young person.
- Viewing, production, distribution and possession of extreme pornographic images.
- Buying or selling stolen goods.
- Inciting religious hatred and acts of terrorism.

Responding to misuse/incidents
The school policies and protocols on child protection, safeguarding and e-safety *must be* followed if any apparent, suspected or actual misuse appears to involve illegal or inappropriate activity:

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.
- Potential radicalisation or extremism.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school's) reputation in some way or are deemed as being inappropriate will be responded to by the senior leadership team.

In the event that any member of staff, is found to be posting libellous or inflammatory comments on social networking sites, this will be addressed by the school in the first instance. If appropriate, disciplinary action will result. However, where necessary, the police will be involved and/or legal action pursued.

The current Criminal Prosecution Service (CPS) guidance *'Guidelines on prosecuting cases involving communications sent via social media'* came into effect on 20 June 2013 and set out the approach that prosecutors should take when making decisions in relation to cases where it is alleged that criminal offences have been committed by the sending of a communication via social media. These guidelines are helpful when used alongside school employment and disciplinary policies in cases where staff misuse may be the issue.