ST.MARK'S CE SCHOOL

ONE SCHOOL - SERVING ALL - THROUGH EXCELLENCE

Social Media and Networking Policy

Policy Statement and Guidelines

Policy Date: Spring 2026

Review Date: Spring 2027

1. Introduction

(i) This document sets out the school's policy on social media and networking. New technologies are an integral part of our lives and are widespread powerful tools which bring new communication opportunities in teaching and learning for pupils and school staff in many ways. It is important that we are able to use these technologies and services effectively but that this should be balanced with protecting our professional

reputation and integrity. With this in mind, all staff working with pupils have a responsibility to maintain public confidence in their ability to safeguard pupils' welfare, and to behave in the best interests of the pupils and the school that they work for. This procedure is also designed to protect staff from possible harassment by a colleague via a social networking site and advise on how to deal with potential inappropriate use.

(ii) This Policy should be read in conjunction with the school's e-safety and digital technology, Acceptable use of ICT, safeguarding, Staff Code of Conduct and any other related policies and should also be read in conjunction with the school's Disciplinary Procedure and staff handbook. If staff fail to adhere to the guidelines set out in this Policy, their conduct could be called into question and may result in disciplinary action being taken against them which could ultimately lead to their dismissal.

(iii) Whilst this Policy has attempted to cover a wide range of situations, it cannot cover all eventualities. Staff using social media and networking sites should avoid any conduct which would lead any reasonable person to question their motives and intentions.

(iv) The School understands that employees have the right to a private life and would respect this so long as employees follow the guidelines set out in this Policy and other documents it refers to. The School expects employees to maintain reasonable standards in their own behaviour such that enables them to maintain an effective learning environment and also to uphold public trust and confidence in them and their profession. Employees should avoid any conduct which is likely to bring the school into disrepute.

(v) Staff are given sufficient training and knowledge to recognise and report potential misuse and use systems relevant to their role.

(vi) The purpose of this policy is to ensure:

- That the school is not exposed to legal risks
- That the reputation of the school is not adversely affected
- That our users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the school.

2. Scope

(i) This Policy applies to all staff who work in the school. This includes all teaching and non- teaching staff. The general principles set out in this policy should also be followed by adults who work at the school but are not employed by the school (i.e. Governors, Volunteers etc).

(ii) For the purpose of the policy, social media and social networking sites are websites by which personal information or opinions can be presented for public consumption and websites which allow people to interact with each other. Examples of social media and social networking sites could be all internet presence including blogs, Facebook, Twitter, Web 2, Bebo, Youtube and MySpace. This list is not exhaustive as new technology is emerging on a daily basis but it seeks to provide examples to

staff. The definition of social networking and media may be widened as new technologies emerge.

(iii) All school representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School's Equality and Diversity Policy.

3. Staff guidelines in relation to social networking and media activity

(i) **Use of Social networking sites in work time**

Use of social networking applications in work time for personal use, is not permitted, unless permission has been given by the Executive Headteacher or someone delegated to give permission on their behalf.

(ii) **Social Networking as part of School Service**

All proposals for using social networking applications as part of a school service (whether they are hosted by the school or a third party) must be approved by the Executive Headteacher or a member of the SLT first.

(iii) Individual Social Networking service

Staff wishing to have a social media presence should make sure that their employer is not identified on this presence unless there is, on an objective assessment, a legitimate reason for doing so and should ensure that comments made are from their own behalf, for example by writing in the first person and using a personal e-mail address as opposed to their employer's e-mail address.

(iv) Social Networking Applications:

Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.

- Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns.
- Must not be used for actions that would put school representatives in breach of school codes of conduct of policies relating to staff.
- Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents.
- Employees should not identify themselves as a representative of the school activity/event unless prior permission has been obtained and agreed with the Executive Headteacher.
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action.

• Where family and friends have pupils in school and there are legitimate family links, please inform the Executive Headteacher in writing. However, it would not be appropriate to network during the working day on school equipment.

• It is illegal for an adult to network, giving their age and status as a child. · If you have any evidence of pupils or adults using social networking sites in the working day, please contact the designated safeguarding lead (pupil) or Executive Headteacher (staff).

Any breaches of this policy will be subject to the school's disciplinary procedures, which may include formal investigation and sanctions up to dismissal. Staff and pupils should report any concerns or breaches promptly to the Executive Headteacher or designated safeguarding lead.

(v) Communication on Social Media

Staff are personally responsible for their communication in social media. This includes any media attachments like photographs or videos. What staff publish on a social media site will be available for any member of the public to read (including parents, members of the Governing Body, colleagues, members of the Local Authority and prospective employers) for a long time. Staff should always think carefully about this when posting personal content.

(vi) Social Media Attachments

Staff should not post any media attachments, such as photographs or videos, which have subjects (pupils/colleagues etc) of the school in them. Anyone wishing to post such items should always speak to the Executive Headteacher in the first instance.

(vii) Social Media Information - Contact

Staff should not place any information regarding their employer, their colleagues, pupils or people they come into contact with as part of their employment on a social networking or media site, without permission from staff member.

(viii) Social Media Information – Personal Information

Staff are advised for their own protection not to put personal information such as home addresses or personal telephone numbers on a social networking or media *site.* Staff must ensure compliance with data protection legislation (e.g., UK GDPR) by not sharing personal data of pupils, colleagues, or parents on social media without explicit consent. Staff should consult the Data Protection Officer if unsure.

4. Staff guidelines in relation to pupil contact

(i) **'Friending' present or past students**

Staff will not interact with any pupil (or past pupil under the age of 18) of the school on a social media or networking site. For example, the school would not think it appropriate for staff to 'friend' a pupil or request that a pupil 'friend' them. If a member of staff receives a request to interact with a pupil

or past pupil under the age of 18, they should inform the Executive Headteacher

(ii) Electronic Communication

All electronic communication with pupils and parents must be conducted through approved school platforms only. Use of personal devices or accounts for school-related communication is prohibited unless explicitly authorised. Staff should use only the school's website, the schools e-mail address or the school's telephone number when communicating with pupils and parents/carers.

(iii) Social Media Comments and Content

Staff should not post remarks or comments on-line or engage in online activities which may bring the school into disrepute.

5. Pupil Guidelines

The school will provide ongoing education to pupils about safe and responsible use of social media, including understanding digital footprints, privacy settings, and how to report concerns.

- No pupil should be accessing social networking sites unless they are at the minimum legal age. This is the guidance from a social media account and a school directive. There is a mechanism on different social media platforms where pupils can be reported via the Help Screen.
- No pupil may access social networking sites during the school working day. • All primary pupil mobile phones must be handed in to the teacher at the beginning of the school day, the Internet capability must be switched off and Secondary must follow the mobile phone policy or it will lead to sanctions as described in the policy.
- No pupil should attempt to join a staff member's area on networking sites. If pupils attempt to do this, the member of staff is to inform the Executive Headteacher. Parents will be informed if this happens and IT Team will take any action as needed.
- No school devices are to be used to access social networking sites at any time of day unless for direct use (i.e. posting school information on the school Facebook page).
- Any attempts to breach firewalls or security measures (including circumventing e-safety and security policies and settings) will result in a ban from using school ICT equipment other than with close supervision.
- Please report any improper contact or cyber bullying to the class teacher in confidence as soon as it happens.
- We have a zero tolerance to cyber bullying.

6. Child Protection Guidance

(i) Disclosure

If the Executive Headteacher 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 their safeguarding policy
- Schools must refer the matter to the LADO who will investigate via Southampton City Council.
- If the disclosure has come from a parent, take normal steps to calm the parent and explain processes.
- If disclosure(s) comes from a member of staff, try to maintain confidentiality. •

The LADO will advise whether the member of staff should be suspended pending investigation after contact with the police (or appropriate authority). It is not recommended that action is taken until advice has been given.

- If disclosure is from a child, follow your normal process in your child protection policy until the police (or appropriate authority) investigation has been carried out.

7. Social media and networking sites and cyberbullying

(i) Staff Cyber-bullying

Staff should never use social media to abuse or bully or otherwise comment about colleagues, pupils, carers of the pupils or anyone associated in the wider context of the school (e.g. member of the Governing Body, Local Authority, sponsor etc). Staff are expected to act respectfully when using social media and to avoid language which may be deemed as offensive to other people. For example, the school would not expect any member of staff to post anything which:

- could be construed as discriminatory
- could be construed as racist
- is untrue or misleading
- engages in criminal activity
- is defamatory about people or organisations

Staff will also share these expectations. Incidents of cyberbullying will be addressed in line with the school's Disciplinary Policy (staff), and Anti-Bullying Policy/ Behaviour policy, ensuring a coordinated approach to prevention, intervention, and support for all parties involved.

(ii) Staff subject of Cyber-bullying *"intervention, and support for all parties involved."*

Staff who feel that they are subject to social media bullying by another member of staff or a pupil should where possible save evidence (e.g. e-mails, screen prints, text messages) and immediately report this to the Headteacher for further investigation. Where the complaint is against the Executive Headteacher, the concern should be raised with the Chair of the Governing Body for further investigation.

(iii) Staff Concerns

Staff who feel that a colleague is not adhering to this policy should report their concerns to the Executive Headteacher for further investigation. Where the complaint is against the Executive Headteacher, the concern should be raised with the Chair of the Governing Body for further investigation.

By adopting the recommended no use of social networking on sites on school premises, St. Mark's School protects themselves from accusations of complicity in any cyber bullying through the provision of access.
Parents should be clearly aware of the school's policy of access to social networking sites.

Where a disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the school.

Once disclosure is made, investigation will have to involve the families. This should be dealt with under the school's adopted bullying and/or behaviour policy.

If parent/carers refuse to engage and bullying continues, it can be referred to the police as harassment.
This guidance can also apply to text and mobile phone bullying and any form of electronic form of bullying.

If a parent/carer is making threats online against a member of school staff, this is counted as bullying. The member of staff must inform the Executive Headteacher immediately and the parent/carer spoken to. Should the situation not be resolved, the police and LA should be informed.

Monitoring and Review

The school will regularly monitor the effectiveness of this Social Media and Networking Policy through staff feedback, incident reports, and periodic review. The policy will be reviewed annually or sooner if required to reflect changes in legislation or technology.