



St Martin's School

Social Media Policy

Introduction

The widespread availability and use of social networking applications bring opportunities to communicate with various groups in new ways. It is recognised that social networking has the potential to play an important part in many aspects of school life, including teaching and learning, external communications and continuing professional development. St Martin's therefore encourages the responsible and professional use of the internet and social media to support educational delivery and professional development.

Whilst recognising the benefits social media brings, this policy sets out the principles designed to ensure that all staff members use social media responsibly so that the confidentiality of students, staff and the reputation of the school are safeguarded. It is essential that pupils, parents and the wider public have confidence in the school's decisions and services. In this context, staff members must always be conscious of the need to keep their personal and professional lives separate. This policy covers personal use of social media as well as the use of social media for official school purposes and outlines the risks to users and the school, as well as the potential consequences of misuse of the internet and social media. St Martin's recognises the need to offer a protection for employees who may be harassed or victimised by other members of the school community due to their professional relationship with the school.

Coverage/Application?

The policy applies to personal media platforms such as networking sites (e.g. Facebook, Googlechat), blogs, microblogs (e.g. X), chatrooms, forums, podcasts, open access, online encyclopaedias (e.g. Wikipedia) and content sharing sites (e.g. Flickr and YouTube). However, this list is not exhaustive and new online platforms are to be considered automatically covered. This policy also applies to online message boards/forums and comments under news items and other articles. The internet is fast moving technology and it is impossible to cover all circumstances or emerging media therefore the principles set out in this policy must be followed closely, irrespective of the medium or platform.

This policy equally applies to all employees including teacher trainees, any other individuals who work for or provide services on behalf of the school and members of the St Martin's community.

Policy Aims

To minimise the reputational, legal and governance risks to the school and its employees, arising from use of social media in both personal and professional capacities.

To enable the safe use of social media for the purposes of communication and engagement.

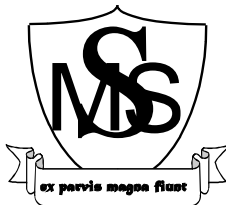
To ensure a consistent approach is applied across the school.

To identify responsibilities of the school and employees in line with all other policies, particularly safeguarding and child protection.

Legal implications

Staff should be aware that there are a number of legal implications associated with the inappropriate use of social media. Liability can arise under the laws of:

- Defamation
- Discrimination
- Human Rights
- Copyright
- Contract
- Protection from harassment



- Criminal harassment - Data protection

For purposes of this policy the term 'public' is used to refer to those outside of the immediate school community (Employees, contractors and pupils) and includes (but not exclusively) parents/carers and ex-pupils.

User responsibilities

All users must be aware that as soon as a post is made online, it is no longer within the private sphere or in the control of the original poster.

If an employee is found to have breached this policy, they may be subject to disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist with the prosecution of the offenders.

Any misuse of social media must be reported promptly to the safeguarding lead or head teacher, whether carried out by pupils, parents/guardians or staff members.

Reporting

Where staff have concerns about e-safety, these should be raised with the Data protection Lead, Safeguarding Lead, Deputy Safeguarding Lead or Headteacher as soon possible.

Advice can also be sought from professional associations and trade unions.

Principles

In all communications, members of the school should:

- a) always be conscious of the need to keep personal and professional lives separate. Staff should not put themselves in a position where there is a conflict between their work and personal interests.
- b) not engage in activities involving social media which may bring St Martin's into disrepute.
- c) not represent their personal views as those of the school on any social medium.
- d) not discuss personal information about students, staff and any other professionals that they interact with as part of their job, on social media.
- e) follow safeguarding principles
- f) be open, honest, ethical and professional;
- g) use jargon-free, plain English in professional communication;
- h) use the method of communication that is most effective and appropriate to the context, message and audience;
- i) be cost effective.

Risks

The school recognises the risks associated with use of the internet and social media and regulates their use to ensure this does not damage the school, its staff and the people it serves. Principal amongst these risks are:

- access to inappropriate material;
- civil or criminal action relating to breaches of legislation;
- cyber bullying by pupils/students;
- damage to the reputation of the school;
- disclosure of confidential information;
- inappropriate behaviour, criticism and complaints from external sources;
- loss or theft of personal data;
- offending behaviour toward staff members by other staff or pupils/students;
- other misuse by staff including inappropriate personal use;



- social engineering attacks - i.e. the act of manipulating people into disclosing confidential material or carrying out certain actions;
- staff members openly identifying themselves as school personnel and making disparaging remarks about the school and/or its policies, about other staff members, pupils or other people associated with the school.
- damage to professional reputations with current and future employers.
- virus or other malware (malicious software) infection from infected sites.

Monitoring

All school systems may be monitored so personal privacy cannot be assumed when using school hardware. St Martin's can monitor the usage of its own internet and email services without prior notification or authorisation from users (staff, contractors and pupils) when justifiable concerns have been raised re: electronic communication. This will be in line with school investigation procedures. St Martin's respects the privacy of its employees. However, postings made on a personal account may attain a wide readership and will therefore be considered public rather than private. Publicly accessible postings may be investigated if there is a suspected breach of this or related policies.

When a public post is reported concerning non-employee members of the school community, this will be investigated and responded to by the school. Further action may be taken to assist with the prosecution of the offenders.

External communication with parents/carers

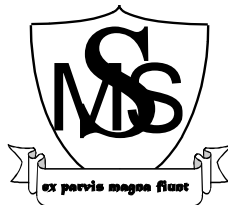
St Martin's has many lines of communication to maintain positive working relationships with parents/carers. These include: letters, telephone calls, emails, face-to-face meetings, the website, Facebook, X, St Martin's Post, progress reports and parents' evenings. Effective communications not only deliver the specific information required, but also enable us to demonstrate our values and ethos. Communication with parents/carers should always reinforce parental support and engagement. Communications will seek to establish open and positive relationships with parents, whilst always ensuring that these relationships are professional. To this end, parents should always be addressed in an appropriate manner using formal mediums of communication i.e. telephone, email, letter. Staff will not communicate with parents/carers or pupils via networking sites, personal devices or e-mail. Where there is a need to communicate directly with parents/carers (i.e. on school trips) staff will do so via the school office, have access to school provided equipment i.e. mobile phones or in extreme circumstances and with prior permission from the proprietor or Headteacher, using a withheld number. Schools may use Facebook and Tweets but this is carefully regulated and not "owned" by individual members of staff. Mrs Wilson and Mr Zucker are the designated members of St Martin's who are trained.

External communication with pupils

Communication with pupils will take place face-to-face or via a staff member's school email address only. A staff member will not communicate with a pupil via their personal mobile phone or using personal email addresses. All communication with pupils will be via a school email, parent email or pre-arranged video conferencing supervised by a home adult.

Personal Use of Social Media

Staff members are strongly encouraged not to identify themselves as staff members of their school in their personal social media platforms. This is to prevent information on these sites from being linked with St Martin's School and to safeguard the privacy of staff members. This does not include professional



networking sites. Staff should also select carefully their social media profile picture as it is an extension to their professional image online.

Staff should not have contact through any social medium with any student from St Martin's School or any other school. Staff are advised not to communicate on social media platforms with ex-students except via professional networking sites for professional reasons. Staff should decline 'friend requests' from students they receive in their personal social media accounts.

Information staff members have access to as part of their employment, including personal information about students and their family members, colleagues and other parties must not be discussed on their personal social media platforms.

Photographs, videos or any of images of pupils or students should not be published on personal social media platforms.

School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media unless pre-approved by school leadership.

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.

Staff are strongly advised to ensure that they set up and regularly review 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 what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information.

Caution should be exercised when using social media, and avoided if possible beyond the school staff WhatsApp group. Where possible, all work related communication should be through school email or contact details held by the school.

Any misuse or abuse of social media must be reported to the designated safeguarding officers or the Headteacher as soon as noticed, especially when concerning a pupil, parent/guardian or employee.

Where a member of staff is a parent/guardian as well as an employee of the school

In cases where staff are also parents connected to the school, they are advised to use professional judgment (in reference to child protection and safeguarding policies) when communicating with children or young people also connected to the school community. Staff should only accept friend requests/communicate with others linked to the school community when there is a genuine need. This relationship should stand up to scrutiny from a professional perspective and should be appropriate. If a concern of safeguarding arises, this should be reported to the designated safeguarding lead in accordance with school policy.

Using social media on behalf of St Martin's

Authorised staff should only use official social media school sites (Teams) for communicating with students, to enable students to communicate with one another or for professional school marketing and recruitment.

Staff should not use personal social media accounts for official school business. Staff must always act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

On school trips staff MUST communicate via the school office or use a school mobile phone, staff should never give out their personal number to parents, carers or pupils. School based staff will be made aware of the implications of using personal devices and will be advised that accessing school communications on personal devices is not an expectation or a condition of employment at the school. St Martin's school provides access to suitable hardware and software where required.



St Martin's website

CST are responsible for maintaining the school website and staff are responsible for its content. There will be regular communication between the administrator and members of the school leadership to monitor and update appropriate content for posting on the school website.

Use of Images

Permissions are sought for images of children used in school produced materials. Clear reference to online usage is made when permissions are requested.

Staff must give permission for their images to be used in school produced materials accessible by members of the public (online or in print), whether controlled by the school or not. Photographs must be checked carefully to ensure that children who are on the restricted list are never shown.

Cyber bullying and Harassment

Cyberbullying is making use of information and communications technology, particularly mobile phones and the internet, to deliberately undermine, humiliate or otherwise cause distress to the person on the receiving end. Staff must not use social media and the internet to attack, insult, abuse or defame anyone - particularly pupils, their family members, colleagues, other professionals, St Martin's or other organisations.

Cyber Bullying and Cyber Harassment, like other forms of bullying and harassment, imply a relationship where an individual has some influence or advantage that is used improperly over another person or persons, where the victim is subjected to a disadvantage or detriment, and where the behaviour is unwarranted and unwelcome to the victim. However, in this case the technological environment has meant that the acts of bullying and harassment now include the use of information and communications technology including email and social networking.

It should be noted that a person does not need to directly experience this form of victimisation in order for it to be classed as cyber bullying/harassment. The fact that a person is unaware that offensive or derogatory comments about them have been placed on websites still fits the criteria of cyber bullying/harassment.

Staff should not personally engage with cyberbullying incidents and should immediately report incidents to the safeguarding lead or Headteacher.

If a member of staff is the victim (receives any threats, abuse or harassment from members of the public through their use of social media), they should keep any records of the abuse and if appropriate, screen prints of messages or webpages with time, date and address of the site and follow reporting procedures. The school will consider it a potential disciplinary matter if users utilise any information and communications technology, in such a way as to bully/harass others in the school, partner organisations, pupils or parents, whether this takes place during or outside of work.

Staff, members of St Martin's community and pupils need to be aware that no matter what the privacy settings on their social media/networking site, inappropriate/derogatory information about a colleague in the school or partner organisations, other pupils or parents, can find its way into the public domain even when not intended.

If a member of staff is the perpetrator of the incident/s the situation will then be investigated and if appropriate, the Disciplinary or Capability Procedure will be followed.

If a pupil is the perpetrator of the incident/s the situation will be initially investigated in line with the school behaviour policy. Where appropriate the police will be consulted.

Where a potential criminal offence has been identified, and reported to the police, St Martin's will ensure that any internal investigation does not interfere with police enquires. Staff who are victims of cyber-



bullying or harassment will be offered support by their line manager and where suitable, occupational health.

Senior Leadership responsibility in relation to Online Bullying and Harassment

St Martin's recognises it has a duty of care to employees to take reasonable steps to provide a safe working environment free from bullying and harassment. For this reason, it is essential that the Senior Leadership Team take appropriate steps to deal with any incident where it is alleged that a staff member has subjected others to abusive or personally offensive emails, phone calls or content on social networking sites such as Facebook, X, or by any other means.

If a Senior Leader is made aware of such an allegation, they will deal with it in the same way as any other incident of bullying or harassment in line with school policies, by investigating the allegations promptly and appropriately and providing the victim with appropriate support to demonstrate that the matter is being dealt with seriously.

Senior Leaders will encourage staff to preserve all evidence by not deleting emails. In addition, logging phone calls and taking screen-prints of websites would all help towards supporting an investigation. If the incident involves illegal content or contains threats of a physical or sexual nature, the Senior Leadership team will advise the employee that they should inform the police.

If such evidence contains indecent images of children, it is an offence to save, send, or alter an image or to show it to anyone else. Therefore, the evidence must be placed in a secure location such as a locked cupboard where others will not be able to see it. In these circumstances the Police will be contacted immediately for advice.

Written by: Mrs Mbah
Ratification date: 22nd May 2024

Ratified by: Governing Body
To be reviewed: May 2025