Social Media Policy

This Policy was reviewed	**Spring Term 2017**
Determined by Governors:	**March 2017**
To be Reviewed:	**Spring Term 2019**

'St Mary's is a Christian School where we aim to
Value – Inspire – Learn and Celebrate Together'

1. Introduction

For the purposes of this policy, social media refers to any internet or intranet based interactive platform, including social networks, internet forums and blogs. Given the rapid expansion of social media, it is impossible to list all possible types. Staff and the wider Academy community, including parents and pupils, should assume that all online activity relating to the school is covered by this policy and should follow these guidelines in relation to any social media that they use.

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. The Academy has this policy in place to deal with any misuse of social media.

All the Academy community are reminded that information they share through social media, even if they are on private spaces, are still subject to copyright, data protection, Freedom of Information legislation, and other legislation.

2. Objectives and Targets

This policy applies to teachers, support staff, governors, volunteers and all who work on the Academy site as well as the wider Academy community including parents and pupils.
The policy takes account of all the appropriate legislation and sets out to:

- Assist those who work with pupils to work safely and responsibly, 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 to those within the Academy community.
- Advise that, in the event of unsafe and/or unacceptable behaviour, disciplinary or legal action (including gross misconduct leading to dismissal for staff) 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.

3. Legal Framework

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, and the Data Protection Act 1998.

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 pupil photographs
- Information divulged in the expectation of confidentiality
- School records containing sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations.

All users should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including Libel and Defamation Acts, Protection from Harassment Act, Criminal Justice and Public Order Act, Malicious Communications Act, Communications Act and Copyright, Designs and Patents Act.

The Academy could be held vicariously responsible for their employees. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex or disability.

4. Action plan

Use of social media within school
Staff and pupils are not permitted to access social media from the school's computers or other Academy provided device at any time unless authorised to do so by a member of the senior management team. The exception is any school social media website or as part of the curriculum. Staff may use their own devices to access their own social media websites while they are in school, outside of session times. Excessive use of social media, which could be considered to interfere with productivity, will be considered a disciplinary matter.

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

Use of social media must not:

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

Use of social media outside of school
The school appreciates that the Academy community uses social media in a personal capacity. However, staff and other members of the Academy community 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 Academy opinion and so could damage our reputation. Opinions offered should not to bring the school into disrepute, breach confidentiality or copyright, or bully, harass or discriminate in any way.

Staff will not invite, accept or engage in communications with parents or pupils from the Academy on any personal social media site unless they have a specific relationship (eg family).

Any inappropriate communication from a member of the Academy community should be reported to the e-safety officer. This could include an addiction to social media.

5. General Considerations

When using social media staff and others must:

- Never share work log-in details or passwords
- Keep personal phone numbers private
- Never give personal email addresses to pupils or parents
- Restrict access to certain groups of people on their social media sites and pages.

Those working with children have a duty of care and are therefore expected to adopt high standards of behaviour to retain the confidence and respect of colleagues and the Academy community both within and outside of school. They should maintain appropriate boundaries and manage personal information effectively so that it cannot be misused by third parties.

Staff must not make 'friends' of pupils at the school, nor should they accept invitations to become a 'friend' of any pupils. Staff should also carefully consider contact with a pupil's family members because this may give rise to concerns over objectivity and/or impartiality. Staff must keep any communications with parents/pupils transparent and professional and should not use personal systems for school 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 management team should be informed so that they can decide how to deal with the situation. 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.

6. Misuse of Social Media

While acknowledging the benefits of social media and the internet it is also important to recognise the risk to the safety and well-being of users. Misuse can be summarised as follows:

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)

7. Disciplinary action

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

The Academy community must be aware of what is considered to be 'criminal' when using social media 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.

- 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:
    - Hard/Soft-core pornography
    - Hate material
    - Drugs
    - Weapons
    - Violence
    - Racism
    - Radicalisation
- 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, radicalisation and acts of terrorism
- Downloading multimedia (music and films) that has copyright attached.

8. Responding to Misuse/Incidents

- If you know the identity of the perpetrator, contacting their parents or, in the case of older children, the young person themselves to ask that the offending content be removed.
- Having kept a copy of the page or message in question report the event to the Academy e-safety officer.
- Use the controls supplied by the site creators to report the misuse. Read and cite the site Terms and Conditions of Use where appropriate to confirm and reinforce your actions.
- Support the victim and if appropriate and they wish to do so, assist them in reporting the incident via the 'Click CEOP' button on the Academy website or on the Child Exploitation and Online Protection website (http://ceop.police.uk).
- If the offending content was authored by someone who contravened the social media site age rules then the social media site must be informed so they can take appropriate action to prevent re-occurrence.
- Any misuse/incidents associated with Academy social media websites are to be reported to the e-safety officer.

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.
  - Radicalisation

- Any actions online that impact on the Academy and can potentially lower the Academy's reputation in some way or are deemed as being inappropriate will always be responded to.
- In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on social networking sites, this will be addressed by the Academy in the first instance. If appropriate, disciplinary action will result. 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 Academy employment and disciplinary policies in cases where staff misuse may the issue.

9. Monitoring and Reviewing

The Academy will monitor the impact of the policy using logs of reported incidents and it will be reviewed by the governors annually, or, in the light of any incidents, significant new developments in the use of the technologies, or perceived new threats.

Signed: …….. Date: …….
Derek Kuziw
Chair of Governors