

# Social Media Policy

“What does the Lord ask of you? To act justly, to love mercy and to walk humbly with your God.”

(Micah 6:8)

## Contents:

### Statement of intent

1. [Key roles and responsibilities](#)
2. [Definitions](#)
3. [Training of staff](#)
4. [Pupil expectations](#)
5. [Social media use - staff](#)
6. [Social media use - pupils and parents / carers](#)
7. [The school blogging rules](#)
8. [Blocked content](#)
9. [Cyber bullying](#)
10. [Be SMART online](#)
11. [Monitoring and review](#)

### Appendices

- a) [Blocked content access form](#)
- b) [Inappropriate content report form](#)
- c) [Contact details for social networking sites](#)
- d) [Mobile phones](#)

## Statement of intent

In our school, our Christian vision shapes all we do. All members of the school community are committed to upholding the St Michael's Church of England Christian values:

- to show love, care and kindness to all in our community
- to value what we have and to share with others
- to enable everyone to achieve their full potential

St Michael's Church of England High School understands that social media is a growing part of life outside of school. We have a responsibility to safeguard our pupils against potential dangers when accessing the internet at school, and to educate our pupils about how to protect themselves online when outside of school.

St Michael's Church of England High School has a commitment to achieving success through partnership. We believe that a three-way partnership between the school, its students and their parents is vital to success and this vision has been drawn up to set out what can reasonably be expected by all concerned.

We are committed to:

- encouraging the responsible use of social media in support of the school's mission, values and objectives
- protecting our pupils from the dangers of social media
- preventing and avoiding damage to the reputation of the school through irresponsible use of social media
- protecting our staff from cyber bullying and potentially career damaging behaviour
- arranging e-safety meetings for parents

Signed by:

_____	Headteacher	Date:	_____
_____	Chair of governors	Date:	_____

**Date adopted** 22<sup>nd</sup> March 2018  
**Review date** January 2021

## **1. Key roles and responsibilities**

- 1.1. The governing board has overall responsibility for the implementation of the Social Media Policy and procedures of St Michael's Church of England High School.
- 1.2. The governing board has responsibility for ensuring that the Social Media Policy, as written, does not discriminate on any grounds, including but not limited to: ethnicity/national origin, culture, religion, gender, disability or sexual orientation.
- 1.3. The governing board has responsibility for handling complaints regarding this policy as outlined in the school's Complaints Procedure Policy.
- 1.4. The Headteacher will be responsible for the day-to-day implementation and management of the Social Media Policy and procedures of St Michael's Church of England High School.
- 1.5. Staff, including teachers, support staff and volunteers, will be responsible for following the Social Media Policy and for ensuring pupils do so. They will also be responsible for ensuring the policy is implemented fairly and consistently in the classroom.
- 1.6. Parents and carers will be expected to take responsibility for the social media habits of their child/children at home.
- 1.7. Parents and carers will be expected to promote safe social media behaviour.

## **2. The school's e-safety team and network manager**

- 2.1. The school's e-safety team consists of:
  - The Headteacher
  - The Deputy Headteacher (Pastoral)
  - The Assistant Headteacher (Facilities and Resources)
- 2.2. The school's network manager is the third party supplier, Agilisys.

## **3. Definitions**

- 3.1. St Michael's Church of England High School defines "social media" as any online platform that offers real-time interaction between the user and other individuals or groups including but not limited to:
  - blogs
  - online discussion forums, such as netmums.com
  - collaborative spaces, such as Facebook
  - media sharing services, such as YouTube
  - 'micro-blogging' applications, such as Twitter
- 3.2. St Michael's Church of England High School defines "cyber bullying" as any use of social media or communication technology to bully an individual or group.
- 3.3. St Michael's Church of England High School defines "members of the school community" as any teacher, member of support staff, pupil, parent/carer of pupil, governor or ex-pupil.

#### **4. Training of staff**

- 4.1. At St Michael's Church of England High School, we recognise that early intervention can protect pupils who may be at risk of cyber bullying or negative social media behaviour. As such, teachers will receive training in identifying potentially at-risk pupils.
- 4.2. Teachers and support staff will receive training on the Social Media Policy as part of their new starter induction.
- 4.3. Teachers and support staff will receive regular and ongoing training as part of their development.

#### **5. Pupil expectations**

- 5.1. Pupils are responsible for following the school rules and will be expected to follow requests from teachers.

#### **6. Social media use - staff**

- 6.1. School social media passwords are kept in the Assistant Headteacher, Facilities and Resource's office. The passwords must never be shared.
- 6.2. The Compliance & Quality Manager is responsible for the school's social media accounts.
- 6.3. Teachers may not access social media during lesson time, unless it is part of a curriculum activity.
- 6.4. The use of smart phone technology is outlined in our Mobile Phone Policy.
- 6.5. Teachers may use social media during their break times.
- 6.6. Members of staff should avoid using social media in front of pupils.
- 6.7. Members of staff **must not** "friend" or otherwise contact pupils or parents/carers through social media.
- 6.8. If pupils or parents/carers attempt to "friend" or otherwise contact members of staff through social media, they should be reported to the Headteacher.
- 6.9. Members of staff should avoid identifying themselves as an employee of St Michael's Church of England High School on social media.
- 6.10. Members of staff **must not** post content online which is damaging to the school or any of its staff or pupils.
- 6.11. Where teachers or members of staff use social media in a personal capacity, they should make it clear that their views are personal.
- 6.12. Teachers or members of staff must not post any information which could identify a pupil, class or the school unless it is an official school capacity.

- 6.13. Members of staff should not post anonymously or under an alias to evade the guidance given in this policy.
- 6.14. Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.
- 6.15. Members of staff should be aware that if their out-of-work activity brings St Michael's Church of England High School into disrepute, disciplinary action will be taken.
- 6.16. Members of staff should regularly check their online presence for negative content via search engines.
- 6.17. If inappropriate content is accessed online, an inappropriate website content report form should be completed and passed on to the Headteacher.
- 6.18. Attempts to bully, coerce or manipulate members of the school community via social media by teachers and members of staff will be dealt with as a disciplinary matter.
- 6.19. Members of staff should not leave a computer or other device logged in when away from their desk, or save passwords.
- 6.20. Staff members should use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.

## **7. Social media use – pupils and parents/carers**

- 7.1. Pupils may not access social media during lesson time, unless it is part of a curriculum activity.
- 7.2. Breaches of this policy by pupils will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to exclusion or prosecution.
- 7.3. Pupils and parents/carers **must not** attempt to “friend” or otherwise contact members of staff through social media. If attempts to contact members of staff through social media are made, they will be reported to the Headteacher.
- 7.4. If members of staff attempt to “friend” or otherwise contact pupils or parents/carers through social media, they should be reported to the Headteacher.
- 7.5. Pupils and parents/carers should not post anonymously or under an alias to evade the guidance given in this policy.
- 7.6. Pupils and parents/carers **should not** post content online which could be seen as damaging to the school or any of its staff or pupils, for example:
  - 7.6.1. statements that could be libellous, as social media is considered to be a publishing platform
  - 7.6.2. statements that could be defamatory to any member of staff
  - 7.6.3. statements that could create safeguarding concerns for any pupils.

- 7.7. Pupils at St Michael's Church of England High School must not sign up to social media sites that have an age restriction above the pupil's age.
- 7.8. If inappropriate content is accessed online on school premises, it **must** be reported to a teacher.
- 7.9. The school will seek legal advice regarding any social media misuse as defined above.

## **8. Blocked content**

- 8.1. The following social media websites are blocked by the network's firewalls:
  - Facebook
  - Instagram
  - Twitter
  - Snapchat
- 8.2. Attempts to circumvent the network's firewalls will result in a ban from using school computing equipment, other than with close supervision.
- 8.3. Inappropriate content that is accessed on the school computers should be reported to Agilisys so that the site can be blocked.
- 8.4. Requests may be made to access erroneously blocked content by submitting a "[blocked content access](#)" form to the Headteacher.
- 8.5. The Headteacher will make the final decision on whether access should be granted to a site.

## **9. Cyber bullying**

- 9.1. At St Michael's Church of England High School, cyber bullying is taken seriously.
- 9.2. Incidents of cyber bullying will be dealt with and reported along the same chain as outlined in the Anti-Bullying Policy.
- 9.3. Staff members should never respond or retaliate to cyberbullying incidents. Incidents should instead be reported as inappropriate, and support sought from their line manager or senior staff member.
- 9.4. Evidence from the incident should be saved, including screen prints of messages or web pages, and the time and date of the incident.
- 9.5. Where the perpetrator is a current pupil or colleague, most cases can be dealt with through the school's own disciplinary procedures.
- 9.6. Where the perpetrator is an adult, in nearly all cases, a senior staff member should invite the victim to a meeting to address their concerns. Where appropriate, the perpetrator will be asked to remove the offensive content.
- 9.7. If the perpetrator refuses to comply, it is up to the school to decide what to do next. This could include contacting the internet service provider in question through their reporting mechanisms, if the offensive content breaches their terms and conditions.

- 9.8. If the material is threatening, abusive, sexist, of a sexual nature or constitutes a hate crime, the school should consider contacting the police.
- 9.9. As part of our on-going commitment to the prevention of cyber bullying, regular education and discussion about e-safety will take place as part of computing and the personal, social and health education (PSHE) curriculum.

## **10. Be SMART online**

- 10.1. We encourage pupils to take a SMART approach to social media behaviour:

**Safe** – do not give out personal information, or post photos of yourself to people you talk to online.

Follow age restriction rules

**Meeting** – do not meet somebody you have only met online. We encourage parents/carers to speak regularly to their children about who they are talking to online

**Accepting** – we advise that pupils only open emails and other forms of communication from people they already know

**Reliable** – we teach pupils about the dangers of believing everything they see online

**Tell** – we encourage pupils to tell a teacher, parent or carer if they see anything online that makes them feel uncomfortable

## **11. Monitoring and review**

- 11.1. This policy will be reviewed by the Headteacher on a three yearly basis.



## Appendix a: Blocked content access form

Blocked website content access request form	
Teacher name:	
Full URL:	
Site content:	
Reasons:	
Risks:	
Approved <input type="checkbox"/> Yes <input type="checkbox"/> No	Reason:

## Appendix b: Inappropriate content report form

<b>Inappropriate website content report form</b>
Teacher name:
Full URLs:
General site content:
Nature of inappropriate content:
Safeguarding issue?
Site blocked Date:



## Appendix c: Contact details for social networking sites

Social networking site	Useful links
Ask. Fm	<a href="#">Terms of service</a> <a href="#">Safety tips</a>
BBM	<a href="#">Rules and safety</a>
Facebook	<a href="#">Rules</a> <a href="#">Report to Facebook</a> <a href="#">Safety Centre</a>
Instagram	<a href="#">Rules</a> <a href="#">Report to Instagram</a> <a href="#">Safety Centre</a>
Kik Messenger	<a href="#">Rules</a> <a href="#">Report to Kik</a> <a href="#">Help Centre</a>
Snapchat	<a href="#">Rules</a> <a href="#">Report to Snapchat</a> <a href="#">Safety tips for parents</a>
Tumblr	<a href="#">Rules</a> <a href="#">Report to Tumblr</a> If you email Tumblr, take a screenshot as evidence and attach it.
Twitter	<a href="#">Rules</a> <a href="#">Report to Twitter</a>
Vine	<a href="#">Rules</a> <a href="#">Contacting Vine and reporting</a>
YouTube	<a href="#">Rules</a> <a href="#">Report to YouTube</a> <a href="#">Safety Centre</a>

## Appendix d: Mobile phone reporting

All UK mobile phone providers have malicious or nuisance call, text or picture message centres set up and have procedures in place to help deal with instances of bullying or abuse. They can change numbers and, where necessary, assist the police in tracing malicious calls.

<b>Service provider</b>	<b>From your mobile</b>	<b>Pay as you go</b>	<b>Pay monthly contracts</b>
O2	4445 or 202	08705 678 678	0870 241 0202
VodaFone	191	03333 040 191	03333 048 069
3	333	08433 733 333	08433 733 333
EE	150	0800 956 6000	0800 956 6000
Orange	150	07973 100 450	07973 100 150
T-Mobile	150	07953 966 150	07953 966 150
Virgin	789	0345 6000 789	0345 6000 789
BT		08000 328 751	08000 328 751