

‘Shine as Lights in the World’



St. Michael's Woolmer Green C of E Primary School

Online Safety & Digital Conduct Policy (including the use of AI)

Including Online Safety Acceptable Use Agreements

Date of review:

Date of next review:

Responsibility:

Classification:

June 2026

July 2027

Full Governing Body

Public

Contents

Introduction	1
Aims.....	1
Responsibilities.....	2
Legislation and Guidance	2
Scope of policy	3
Policy and procedure.....	3
Curriculum	6
Artificial Intelligence (AI).....	7
Staff and Governor Training	9
Working in Partnership with Parents/Carers	9
Records, monitoring and review	10
Appendices of the Online Safety Policy	11
Appendix A - Online Safety Acceptable Use Agreement - Staff, Governors and Student Teachers	12
Appendix B – Pupil Online Safety Acceptable Use Agreement for St. Michael’s School	15
Appendix C - Online safety policy guide - Summary of key parent/carers responsibilities.....	17
Appendix D - Guidance on the process for responding to cyberbullying incidents.....	18
Appendix E - Guidance for staff on preventing and responding to negative comments on social media.....	19

Introduction

St. Michael's Woolmer Green School recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. A pupil's future success may, in part, depend on their digital skills, their use of emerging technologies such as artificial intelligence (AI) and their online reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

Aims

St. Michael's aims to:

- Have robust processes in place to ensure the online and digital safety and security of pupils, staff, volunteers and governors
- Identify and support groups of children that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety and digital conduct which empowers us to protect and educate the whole school community in the use of technology, including personal devices, mobile phones, school-issued devices and emerging technologies such as artificial intelligence (AI)
- Promote the safe, responsible and ethical use of AI by ensuring students and staff understand its capabilities and limitations, use it within a clear framework that protects the integrity of pupil work and academic honesty, safeguard personal and school data, remain alert to potential harms, and develop the confidence to use AI appropriately to enhance learning and life beyond school
- Establish clear mechanisms to identify, intervene and escalate incidents where appropriate.

The 4 categories of risk

Our approach to online safety and digital conduct is based on addressing the following categories of risk outlined in Keeping Children Safe in Education (KCSIE):

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including AI-generated deepfakes and fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young people with the intention to groom or exploit the user.

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images, sharing explicit images, misuse of AI, and online bullying.

Commerce – risks such as online gambling, inappropriate advertising, phishing, sextortion and/or financial scams, including those that may exploit AI.

Responsibilities

The Headteacher and Governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety lead in this school is the Headteacher.

All breaches of this policy must be reported to Jan Martin.

All breaches of this policy that may have put a child at risk must also be reported to the Designated Safeguarding Leads DSLs; Jan Martin, Claire Pulham, Claire Woods and James Lawson.

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount, and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#) and its advice for schools on:

- [Teaching Online Safety](#) in schools
- [Preventing & Tackling Bullying](#) including cyber bullying
- [Relationships and Sex Education](#) (RSE) and Health Education
- [Searching, Screening & Confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and [The Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#) which has given teachers stronger powers to tackle cyber-bullying by, if necessary deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The section on artificial intelligence (AI) reflects good practice guidelines/recommendations in the following publications:

- [AI regulation white paper](#), published by the Department of Science, Innovation and Technology and the Office for Artificial Intelligence
- [Generative artificial intelligence](#) (AI) and data protection in schools published by the DfE

It also meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments
<https://www.legislation.gov.uk/ukxi/2020/1586/made>
- [Data Protection Act 2018](#)

Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities.

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe in Education, GDPR, health and safety, home–school agreement, and behaviour policies.

Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use the internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff and Governors should use a school email account or Governor Hub for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Where applicable, pupils should use school approved accounts on the school system for educational purposes. Where required, parent/carer permission will be obtained for the pupil account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to the Headteacher/Business Manager.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect.

Users must not:

- Reveal or publicise confidential or proprietary information.
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school.
- Use the school's hardware and Wi-Fi facilities for running a private business.
- Intimidate, threaten or cause harm to others.
- Access or interfere in any way with other users' accounts.
- Use software or hardware that has been prohibited by the school.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an

expectation that access is pre-planned, risk assessed and recorded, and permission given by the Headteacher.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of pupils are only stored on the school's agreed secure networks which is cloud-based services. Rights of access to stored images are restricted to approved staff as determined by the Headteacher. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly from mobile devices.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in **staff only areas** and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers may not use personal mobile phones and devices in school unless otherwise informed, e.g. for class assemblies and sports day. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the school. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Pupils are not allowed to bring personal mobile devices/phones to school, unless with permission in Years 5 and 6 for the purpose of walking home independently. These will be switched off and handed into the school office, to be collected after school (see mobile devices guidance). Under no circumstance should pupils use their personal mobile devices/phones to take images of

- any other pupil
- any member of staff

The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Personal mobiles can be used to access school emails and data as we have a closed, monitorable system set up by the school for use on a personal device. Personal mobiles may be used to access

authenticator apps to use school platforms such as CPOMs.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with the Headteacher before they are brought into school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSLs and the Headteacher. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive age-appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. The PSHE curriculum, Relationships and Health Curriculum, through Jigsaw as well as the Computer Curriculum, taught through Purple Mash and Internet Safety Days are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives) Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversations

Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.

- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- How the law can help protect against online risks and abuse

Artificial Intelligence (AI)

We follow the 5 principles set out in the white paper:

REGULATORY PRINCIPLE	WE WILL ...
Safety, security and robustness	• Ensure that AI solutions are secure and safe for users and protect users' data • Ensure we can identify and rectify bias or error • Anticipate threats such as hacking
Appropriate transparency and explainability	• Be transparent about our use of AI, and make sure we understand the suggestions it makes
Fairness	• Only use AI solutions that are ethically appropriate, equitable and free from prejudice – in particular, we will fully consider any bias relating to small groups and protected characteristics before using AI, monitor bias closely and correct problems where appropriate
Accountability and governance	• Ensure that the governing board and staff have clear roles and responsibilities in relation to the monitoring, evaluation, maintenance and use of AI
Contestability and redress	• Make sure that staff are empowered to correct and overrule AI suggestions – decisions should be made by the user of AI, not the technology • Allow and respond appropriately to concerns and complaints where AI may have caused error resulting in adverse consequences or unfair treatment

Approved use of AI

We are committed to helping staff and governors reduce their workload. Generative AI tools can make certain written tasks quicker and easier to complete but cannot replace the judgement and knowledge of a human expert.

Whatever tools or resources are used to produce plans, policies or documents, the quality and content of the final document remains the professional responsibility of the person who produced it.

Any plans, policies or documents created using AI should be clearly attributed. Any member of staff or governor using an AI-generated plan, policy, or document should share it only with other members of staff or governors for use if they are confident in the accuracy of the information, as the content remains the professional responsibility of the person who produced it.

Always consider whether AI is the right tool. Just because the school has approved its use doesn't mean it will always be appropriate.

Given how rapidly AI is evolving, this is a living document that is updated as and when we come across a new AI tool we would like to approve for our school, along with the approved uses for each tool. This list will be regularly updated to reflect tools used within the school.

Approved tools	Approved uses
Oak Academy AI lesson planner	Lesson planning
Co-Pilot and Gemini	Document writing, lesson planning, making resources, and image creation
Teachmate	Specifically designed educational resources to help with all areas in education
Canva and DALL-E	Used for the creation and editing of images, creating lesson resources and slides for lessons
Claude	Write, edit, and create content Analyse text and images

This list does not include existing programs used by the team that have recently/plan to include AI features, such as Outlook, Teams and Office. As these new tools are developed and added, the same provisions and expectations will apply to them, so they are used appropriately.

AI is also used to support our use of SEND student including (but not limited to):

- Text simplification
- Alternative explanations
- Visual support
- Lesson resources such as word banks and frames

Educating pupils about AI

Here at St Michaels Primary School, we acknowledge that pupils benefit from a knowledge-rich curriculum that allows them to become well-informed users of technology and understand its impact on society. Strong foundational knowledge will ensure that pupils develop the right skills to make the best use of generative AI.

Within both the computing and PSHE curriculum, pupils are taught about the potential benefits of using AI tools to aid their learning, while also covering subjects such as:

- Creating and using digital content safely and responsibly
- The limitations, reliability and potential bias of generative AI
- How information on the internet is organised and ranked
- Online safety to protect against harmful or misleading content

Use of AI by pupils

We recognise that AI has many uses to help pupils learn. Pupils may use AI tools:

- As a research tool to help them find out about new topics and ideas (Such as Google's inbuilt AI summary on searches)
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images

All AI-generated content must be properly attributed and appropriate for the pupils' age and educational

needs.

AI may also lend itself to cheating and plagiarism. To mitigate this, pupils may not use AI tools:

- During assessments
- To write class activities, where AI-generated text is presented as their own work

This list of AI misuse is not exhaustive.

Where AI tools have been used as a source of information, pupils should reference their use of AI. The reference must show the name of the AI source and the date the content was generated.

Pupils must consider what is ethical and appropriate in their use of AI and must not:

- Generate content to impersonate, bully or harass another person
- explicit or offensive content
- Input offensive, discriminatory or inappropriate content as a prompt

Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

Staff will be offered regular opportunities for relevant CPD as appropriate and efforts made to ensure staff are kept up to date with developments in AI, and how they will be able to develop and improve their practice on a regular basis.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation or volunteers working with children and based on the school premises are also provided with a copy of the online safety policy.

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy.

Guidance is provided for occasional visitors, volunteers and parent/carers helpers (Appendix E).

Working in Partnership with Parents/Carers

The school works with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Parents/carers are asked on an annual basis to read, discuss and update the relevant consents

sections on Arbor. A summary of key parent/carer responsibilities will also be provided and is available in Appendix F. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities.

Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly to ensure they are effective and that the risks to pupils and staff are minimised. Senso is used to alert DSLs to inappropriate words used across many programs i.e. word/web searches. This is monitored by James Lawson (DSL)

All breaches of this policy must be reported, and all reported incidents will be logged and dealt with in line with this policy and our pupil behaviour policy. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported in CPOMs.

If there is a breach of this policy by staff, this will be dealt with in line with our staff code of conduct. Where disciplinary action is appropriate, it may be taken whether the breach occurs:

- During or outside of working hours
- On an individual's own device or a school device
- At home, at school or from a remote working location

Staff members will be required to co-operate with any investigation into a suspected breach of this policy. This may involve providing us with access to:

- The generative AI application in question (whether or not it is one authorised by the school)
- Any relevant passwords or login details

You must report any breach of this policy, either by you or by another member of staff, to the headteacher immediately.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

AI technology, and the benefits, risks and harms related to it, evolve and change rapidly. Consequently, this policy is a live document that must be kept updated when there is a significant change to either AI use by the school or the associated risks of AI usage.

This policy will also be regularly reviewed and updated to align with emerging best practices, technological advancements and changes in regulations.

The policy will be shared with the full governing board at least annually.

All teaching staff are expected to read and follow this policy. The headteacher is responsible for ensuring that the policy is followed.

The computing subject lead and the senior leadership team (SLT) will also monitor the effectiveness of AI usage across the school.

We will ensure that members of the school community are kept up to date on the use of AI technologies for educational purposes. As part of our regular surveys, feedback from pupils, parents/carers and staff will be considered in the ongoing evaluation and development of AI

use in school.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

This Online Safety and Digital Conduct Policy is linked to our:

Data protection policy

Behaviour policy

Staff code of conduct

Marking and feedback policy

Appendices of the Online Safety Policy

- A. Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff)
- B. Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers
- C. Requirements for visitors, volunteers and parent/carers helping working in the school (working directly with children or otherwise)
- D. Online Safety Acceptable Use Agreement Primary Pupils
- E. Online safety policy guide - Summary of key parent/carers responsibilities
- F. Guidance on the process for responding to cyberbullying incidents
- G. Guidance for staff on preventing and responding to negative comments on social media

Appendix A - Online Safety Acceptable Use Agreement - Staff, Governors and Student Teachers

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff, student teachers and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the Headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the DSLs and a written account put on CPoms.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the Headteacher.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils. This includes contact with former pupils, especially those known as 'vulnerable' young people up to the age of 25.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member. We have a supply login for visiting teachers.

Data protection

I will follow requirements for data protection as outlined in GDPR policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the headteacher or governing body
- Personal or sensitive data taken off site must be encrypted

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses or governor hub for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

I will only access secure school information from personal devices when in school or through our closed, monitorable system that has been set up by the school.

Additional hardware/software

I will not install any hardware or software on school equipment without permission.

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the DSLs

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom this will include the acceptability of other material visible, however briefly, on the site. I will not free surf the internet in front of pupils. I will also check the appropriacy of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with a member of the Senior Leadership Team.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSL. A school-owned device should be used when running video-conferences.

User Agreement

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Agreement will be given online at the start of each academic year or when a new member of staff joins the school.

Appendix B – Pupil Online Safety Acceptable Use Agreement for St. Michael's School

Shine as Lights in the World **My Online Safety Rules**

- I will uphold the vision and values of our school
- I will only use school IT equipment for activities agreed by school staff.
- I will not use my personal email address or other personal accounts in school
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.
- In school I will only open or delete my files when told by a member of staff.
- I will not tell anyone other than my parents/carers my passwords. Teachers will know the passwords of children for school use of programs. I will not use other people's usernames or passwords to pretend to be them online.
- I ensure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.
- I will not give out my own or other people's personal information, i.e. name, phone number, address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that some personal devices are allowed in school and some are not, and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.
- I understand my behaviour in the virtual classroom should mirror that in the physical classroom
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all pupils to be safe and responsible when using any IT. It is essential that pupils are aware of online risk, know how to stay safe and know where to go to report problems and access support.

Pupils are expected to read and discuss this agreement with you and then sign below to show they will follow the terms of the agreement.

Please can you update your consents on Arbor to show that you and your child have read and understood this agreement.

Parent(s)/Carer(s) agreement

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or to post material that may bring the school or any individual within it into disrepute.

Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents.

I/we also agree not to use personal mobile phones and devices in the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, they must be switched off and out of sight.

Appendix C - Online safety policy guide - Summary of key parent/carers responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.
- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carers is on school premises but not in a designated area, their phone/s must be switched off and out of sight.
- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.
- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.
- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.
- Any parent/carers, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.

User Agreement

I/We agree to follow this Acceptable Use Agreement and to support online safety throughout the school. Please confirm in the permissions section of Arbor.

Please see the full online safety policy in the policies section on the school website.

Appendix D - Guidance on the process for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix E - Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix F (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts

As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the headteacher will need to follow the school's safeguarding procedures.

If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints

Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;
- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.