Saint Michael's CE High School

A Church of England Academy

Therefore, choose

Online Safety Policy

Responsibility to present to Headteacher	Deputy Head
Approval	Ethos, Staffing & Wellbeing Committee October 2025
Next Review	Ethos, Staffing & Wellbeing Committee October 2026
Statutory	(Supplements Child Protection Policy and Procedures (S))
Required on school website	No

ST MICHAEL'S CHURCH OF ENGLAND HIGH SCHOOL

A BRIEF SUMMARY OF OUR CHRISTIAN VISION

Our motto is **'Therefore choose [life]'** from Deuteronomy.

We understand this to mean growing in **body, mind and spirit**, so that all who learn and work here may flourish, experiencing the joy and hope of '**Life in all its fullness'**.

This is further explained in our Mission Statement,

'As a vibrant learning community
we choose to serve God,
pursue excellence
and celebrate the uniqueness of each individual.'.

Contents

1. Background and Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other e.g. School Synergy, Office 365, Moodle. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school Online Safety policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers Online-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy, and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

The Department for Education categorises the dangers above into four areas of risk (The 4Cs):
Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Misinformation, disinformation and conspiracy theories.
Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams."

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (e.g., behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience and raise awareness of the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguarding to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The online safety policy that follows explains how we intend to do this, whilst also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

The school will monitor the impact of the policy using:

- Internal monitoring data for network activity
- Internet monitoring which is done by Sophos and managed by Atbec
- Online Safety Log – *wellbeing.*
- Pupil managers logs on incidents
- Monitoring logs of internet activity where appropriate (including sites visited)
- Captures of inappropriate language and images through keystrokes

2. Legislation and Guidance

This policy applies to all members of the school community who have access to and are users of school ICT systems, both in and out of school.

This policy also recognises relevant obligations under the Online Safety Act 2023, including duties around harmful and illegal content, reporting systems, and governance oversight.

It includes the Department for Education's updated Filtering and Monitoring Standards (2025), requiring schools to evidence annual reviews of their technical controls.

This policy has been updated to reflect Keeping Children Safe in Education (KCSIE) September 2025, which replaces earlier versions.

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 and tackling bullying and online-bullying: advice for headteachers and school staff

- Searching, screening and 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 online-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of online-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

3. Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

Governors
All governors will:
- Ensure that they have read and understood this policy
- Agree and adhere to the terms of the Digital Usage Policy
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because it is recognised a single approach may not be suitable for all children in all situations, and a more personalised or contextualised approach may be more suitable.
- Governors must ensure oversight includes compliance with the Online Safety Act 2023 codes of practice, KCSIE 2025, and DfE Filtering and Monitoring Standards (2025).

Headteacher and Senior Leadership Team:
The Headteacher is responsible for ensuring the safety (including online safety) of members the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Coordinator.

The Headteacher & Senior Leaders are responsible for ensuring that the Online Safety Coordinator receives regular and up-to-date CPD to enable them to carry out their online safety role, including the training of other colleagues, as relevant.

The Headteacher & Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

DSL's and pastoral team:

Details of the school's DSL and wellbeing team are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT network manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately
- Ensuring that any incidents of online-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher /governing board
- Give advice to colleagues through School Improvement and Wellbeing meetings about appropriate use of technology, privacy settings etc
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Ensures that all staff are aware of the procedures they should advise pupils to follow if there is an online safety incident taking place
- The DSL must consider safeguarding risks arising from AI-generated content such as deepfakes, misinformation, grooming through chatbots, and algorithm-driven targeting.
- Liaises with school ICT technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety assemblies, worships, parent presentations etc.
- To provide top tips for parents within newsletters and on Social Media
- Advertise, present and organise online safety presentations for parents
- Raise awareness of Online Safety during the week of safer internet day

ICT Network Manager/Technical staff:
The ICT Network Manager is responsible for ensuring:

- That the school's ICT infrastructure has an appropriate level of security and procedures are reviewed regularly to assess effectiveness. Such systems should ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- That users may only access the school's networks through a properly enforced password protection policy
- Annual reviews of filtering and monitoring are carried out against DfE standards and that evidence is documented for governors and Ofsted.
- The school's filtering policy is maintained and run by Abtec and we follow their guidance on web filtering
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network / email is regularly monitored in order that any misuse / attempted

misuse can be reported to the ICT Network Manager / Senior Leader for investigation
- That monitoring software / systems are implemented and updated as agreed in school policies
- Liaise with Abtec to block any inappropriate websites which come to their attention

All Teaching and Support Staff:
Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices within school
- They have read, understood and signed the school Staff Digital Technologies Usage Agreement (Appendix 3)
- They report any suspected misuse or problem to the Online Safety Coordinator / Pupil Manager / Form Tutor /Senior Leader for investigation
- They respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, using the school's safeguarding procedure
- Digital communications with pupils (email/Virtual Learning Environment (VLE)/Teams) should be on a professional level and must be only carried out using official school systems (school email account only should be utilised)
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They are aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices
- They act as good role models in their use of ICT, the internet and mobile devices, including in their use of email and Microsoft Teams
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- They are properly "logged-off" at the end of any session in which they are using personal data
- They check devices are empty of personal information, details, images and videos if sharing devices with pupils
- They support any investigations of pupil devices by the DSL or police into online-bullying or abuse which may occur in school

Pupils

- Are responsible for using the school ICT systems in accordance with the Digital Technologies Usage Agreement (Appendix 2), which they will be expected to agree to before given access to the school system
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices, they should also know and understand school policies on the taking / use of images and on online-bullying
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers
Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way

Parents and carers will be responsible for:

- Accessing the school website / VLE / on-line student records in accordance with the relevant school Digital Technologies Usage Agreement.
- Attending the Wellbeing evening is optional, but advised

4. Education & Training

Staff

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including online-bullying and the risks of online radicalisation
- All staff members will receive refresher training as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings)
- Such training will make staff aware that technology is a significant component in many safeguarding and wellbeing issues and that children are at risk of online abuse
- Training will also highlight online peer-on-peer abuse, for example through abusive messages, non-consensual sharing of nude and semi-nude images and sharing of abusive images.
- Staff training will now include awareness of generative AI, deepfake pornography, scams, algorithmic grooming, and the harmful content categories defined under the Online Safety Act.

Training will be offered as follows:

- ICT Network Manager will provide advice / guidance / training as required to individuals as required
- They will also attend the 'New To School' meetings to ensure all new staff fully understand the school Online Safety policy and Digital Technologies Usage Agreement within their induction
- The Deputy Headteacher will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by BECTA / LA and others

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in Online Safety is therefore an essential part of the school's Online Safety provision.

Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience, whilst using social media and game consoles in particular. Online Safety education will be provided in the following ways:

- A planned Online Safety programme should be provided as part of ICT & Living Education
- Key Online Safety messages should be reinforced by the Online Safety Coordinator, as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils will be supported to develop digital resilience in environments shaped by AI, including recognising misinformation, manipulated media, and scams.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil Staff Digital Technologies Usage Agreement (Appendix 2) and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should also be reminded how to report any online safety incidents through school

Online Safety is a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Through Living Education and other lessons, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Parents / Carers

Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. They will receive updated workshops and communication materials on AI risks, harmful content, and age assurance tools.

Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Tanya Byron Report).

The school will therefore take every opportunity to help parents understand these issues through:

- Parents' Wellbeing evenings
- Consultation evenings
- Top Tips in the Newsletter and on the schools Social Media page
- Website – Online Safety page (under Wellbeing)
- Moodle (VLE) – There is a Parental Online Safety page
- Information about national / local online safety campaigns / literature

5. Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the DfE Filtering and Monitoring Standards.
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located
- All users will have clearly defined access rights to school ICT systems
- Details of the access rights available to groups of users will be recorded by the ICT Network Manager and ICT Team and will be reviewed, at least annually
- All users will be provided with a username and password by the ICT Team
- The "master / administrator" passwords for the school ICT system, used by the ICT Network Manager must also be available to the Headteacher or other nominated senior leader
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school maintains and supports a managed filtering system (Senso)
- The school has provided enhanced user-level filtering through the use of Sophos provided and supported by Abtec
- Staff members can request access to websites by raising an ICT Helpdesk ticket through Synergy with a request and reason (this can be done when visiting the restricted website)
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Digital Technologies Usage Agreement
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager (or other relevant person)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, handheld devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- The school infrastructure and individual workstations are protected by up-to-date virus software
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system
- The Digital Technologies Usage Agreement (see appendices) cover the extent of personal use that users (Staff / Pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school

6. Communications

- The official school email service may be regarded as safe and secure and is monitored
- Staff and pupils should therefore be encouraged to use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE, Teams etc) must be professional in tone and content
- These communications should only take place on official school systems. Personal email addresses, text messaging or public chat / social networking programmes **must not** be used for these communications
- Pupils will be provided with individual school email addresses for educational use only
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details
- They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

7. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.

However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution, and publication of those images
- Those must be taken on school equipment
- Digital images/ video should be removed or deleted from the equipment as soon as possible and should only be stored on school equipment and for the minimum period of time necessary
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers is obtained before photographs of pupils are published on the school website

8. Online-bullying

8.1 Definition

Online-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power (see also the school behaviour policy).

8.2 Preventing and addressing online-bullying

To help prevent online-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss online-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss online-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover online-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on online-bullying, its impact and ways to support pupils, as part of safeguarding training

The school also send inform parents/carers on online-bullying so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of online-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

8.3 Examining electronic devices

The headteacher and members of the pastoral team can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- If the search is not urgent, they will seek advice from the DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, the Headteacher and DSL will decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, the headteacher/DSL will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, we may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour for learning policy

8.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Pupils will be taught to critically evaluate AI-generated material, including misinformation and biased outputs.

Teachers introducing AI into lessons must conduct a risk assessment before use, considering safeguarding, data protection, and educational value.
Staff and pupils must not upload sensitive or personal data to AI platforms.

We will treat any use of AI to bully pupils in line with our Behaviour for Learning policy.

Staff are aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by school.

1. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 2 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 2 to 3.

2. Pupils using mobile devices in school

Pupils may bring mobile devices into school but they must be switched off and out of site whilst on school premises.

11. Staff using work devices outside of school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords must have a minimum of 12 characters with at least 1 capital letter, 1 number and 1 special character
- Making sure the device is locked if left inactive for a period of time
- Not sharing the device among family or friends
- Staff members must use the device via the terms set out in the Staff Digital Technologies Usage Agreement. (Appendix 2).
- Work devices must be used solely for work activities
- If staff have any concerns over the security of their device, they must seek advice from the ICT Network Manager or ICT Team

12. Responding to incidents of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the Behaviour for Learning Policy. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

All incidents where illegal material (or could be considered) has been accessed or an attempt has been made to access such material will be referred to the police, Headteacher and Governors as appropriate. Sanctions imposed could include a warning, suspension or removal of network access, or disciplinary procedures.

Governors will receive at least annual assurance reports on online safety incidents, filtering and monitoring, and curriculum coverage.

The school provides clear and accessible reporting routes for pupils, parents, and staff to raise concerns about harmful online content, in line with the Online Safety Act 2023.

Links with other policies

Anti-bullying policy
Behaviour for Learning policy
Relationship and Sex Education policy
Remote Learning policy
Child Protection and Safeguarding policy

Appendix 1. Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at Certain Times	Acceptable for Nominated	Unacceptable	Unacceptable and Illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals, or comments that contain or relate to:	Child sexual abuse images				✓	✓
	Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation				✓	✓
	Adult material that potentially breaches the Obscene Act in the UK				✓	✓
	Criminally racist material				✓	✓
	Pornography				✓	
	Promotion of any kind of discrimination				✓	
	Promotion of any kind of racial or religious hatred				✓	
	Threatening behaviour, including the promotion of physical violence/mental harm				✓	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites, or other mechanisms that bypass the filtering or other safeguards employed by the school					✓	
Uploading, downloading, or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					✓	
Creating/propagating computer viruses or other harmful files					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet					✓	
Registering for a social media account with a school email					✓	

Appendix 2: Pupil Digital Technologies Usage Agreement – Pupils
A copy is also in personal organisers

Pupil Digital Technologies Usage Agreement

Networks
• All information and communications technology is owned by the school and is made available to pupils to further their education - do not abuse this. • The school reserves the right to examine or delete any files that may be held on its systems. • Access to the systems should be made through an authorised account and password, which should not be shared with any other person. • Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems is forbidden. • Use of the systems to access unsuitable materials of a sexual, racist or bullying nature or any other kind of offensive material is forbidden. • Pupils are not to store personal data upon school systems. • Please do not unplug or swap mice and keyboards from one computer to another. Tell a member of staff if equipment isn't working.

Internet and E-mail
• The school reserves the right to monitor all Internet sites and content visited. Visits to inappropriate sites and content by pupils will be notified to the Designated Safeguarding Lead for action. • The school reserves the right to monitor all e-mail activity. • All Internet activity should be appropriate to the curriculum requirements of pupils – no access to social media content. • Where work is protected by copyright, do not download or distribute copies (including music and videos). • School e-mail should not be used for personal use.

Teams, Moodle, Synergy and other online platforms
• The use of forums, private messaging, journals, blogs and professional walls must be limited to school purposes. • The language and content used within these facilities should be appropriate to the task. • Work uploaded or used on Teams, Moodle, Synergy and other online platforms must be of a professional nature and relevant to the task. • Inappropriate use, for example using these facilities as a means to target others, will result in the Headteacher and parents being informed and the pupils involved will be locked out of the system and the relevant disciplinary procedure will be applied.

Pen drives and removable media

- Pen drives and removable media/storage is blocked to protect against the spread of viruses. This is for security to prevent anything malicious infiltration the school systems. Using pen drives is also insecure for the protection of data. Data could be accessed, stolen or lost and not be recoverable. Data should be saved to OneDrive and Teams. This is secure and backed up.

In summary

- Do not use the technology to harm other people or their work.
- Do not view, save, send or display offensive messages or images.
- Do not share your passwords with anyone – see an ICT technician if you need a new password.
- Do not waste limited resources such as paper, ink/toner or storage space.
- Notify a member of staff immediately if, by accident, you encounter inappropriate materials.
- Notify a member of staff immediately if equipment is not working, do not attempt to fix this.

This statement is provided to all pupils by the system on login to a school device which requires accepting to allow access to the system:

All pupils accept the Pupil Digital Technologies Usage Policy when they join St Michael's CE High School. This Policy applies to all pupils. Your use of St Michael's CE High School network means that you accept and agree to abide by every part of the Pupil Digital Technologies Usage Policy.

The Pupil Digital Technologies Usage Policy in personal organisers must be signed by pupils as part of the Home School Agreement.

Appendix 3: Digital Technologies Usage Agreement – Staff

A digital copy is sent to staff via Microsoft Forms

Staff Digital Technologies Usage Agreement

This policy is to protect all parties namely the school, pupils and staff. By signing this agreement, you understand that if you fail to comply with this "Digital Technologies Usage Agreement", you could be subject to disciplinary actions including a warning, suspension, a referral to Governors and/or Local Authority and in the event of illegal activities the involvement of the police.

Networks

- All information and communications technology is owned by the school and is made available to staff and pupils to further assist with education, and for staff to develop curriculum material, management and administration.
- The school reserves the right to examine or delete any files that may be held on its systems.
- Access to the systems should be made through an authorised account and password, which should not be shared with any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems is forbidden.
- Use of the systems to access unsuitable materials of a sexual, racist or bullying nature or any other kind of offensive material is forbidden.
- Staff are advised not to store personal data upon school systems.

Internet and E-mail

- The school reserves the right to monitor all Internet sites and content visited. Visits to inappropriate sites and content by teachers will be notified to the Designated Safeguarding Lead for action.
- The school reserves the right to monitor all e-mail activity.
- All Internet activity should be appropriate to the curriculum requirements of pupils and staff.
- Staff are requested not to input personal data e.g. bank details onto any school laptop or other IT equipment.
- Use of the Internet for personal shopping is forbidden during school hours.
- School will not be held responsible for misuse of personal data obtained from current or former school property by any third party.
- Use of the Internet for financial gain, gambling, political purposes or advertising is forbidden.
- All e-mail communication with parents/carers, pupils or colleagues must be via school e-mail accounts only.
- Users are responsible for all e-mails sent and for contacts made that may results in e-mails been received.
- When using the school e-mail, school website or any form of social media, good professional levels of language and content shall apply. All information posted should be in a formal, courteous and professional tone. All offensive words of any description are forbidden. All communications shall comply with good equal opportunities and non-discriminatory practices. Ensure no information posted would bring the school's reputation into disrepute.
- Where work is protected by copyright, do not download or distribute copies (including music, pictures and videos).
- School e-mail should not be used for personal use.

Teams, Moodle, Synergy and other online platforms
• The use of forums, private messaging, journals, blogs and professional walls must be limited to school purposes. • The language and content used within these facilities should be appropriate to the task. • Work uploaded or used on Teams, Moodle, Synergy and other online platforms must be of a professional nature and relevant to the task. • Inappropriate use, for example using these facilities as a means to target others, will result in the Headteacher and Governing Body being informed, the member of staff involved will be locked out of the system and the relevant disciplinary procedure will be applied.

Staff Devices/Laptops
• As part of our whole school ICT policy in managing Cyber Security controls, there are some configuration settings applied to staff laptops. • The desktop background should not be changed. All staff should use the same background to represent the school's ethos. • It is advisable that only shortcuts are saved to the desktop and not data. Please save data to OneDrive and Teams. This is secure and backed up. • All devices are owned by the school and are made available to staff to enhance their learning and teaching, planning, curriculum material, management and administration. • Microsoft Edge is to be used as the web browser due to security controls. Google Chrome or other web browsers cannot be protected with the same security as it's not a Microsoft product. Google Chrome or other web browsers should not be used as these cannot be made secure by central policies in the same way that Microsoft Edge can be. • Please do not label or place stickers on your laptop or charger other than your name or initials. The reason for this is that from time to time we need to repair laptops and chargers and sometimes a different one will be provided. It can be difficult to remove labels and stickers and we may need to give these to another member of staff. If you require a name label for your charger and/or laptop, please request this via Synergy ICT Helpdesk. • Staff should not install any software. Office 365 is installed. Smart Notebook can be installed on request as we have limited licences. If you require software, please raise a Synergy ICT Helpdesk ticket. The ability to install software is unavailable for staff as all software needs to be managed by central policies and we need to ensure it's the latest version so that each device is secure and free from vulnerabilities.

Pen drives and removable media
• Pen drives and removable media/storage is blocked to protect against the spread of viruses. This is for security to prevent anything malicious infiltration the school systems. Using pen drives is also insecure for the protection of data. Data could be accessed, stolen or lost and not be recoverable. Data should be saved to OneDrive and Teams. This is secure and backed up.

I have read, understand and agree to follow the guidelines within this document during my employment at Saint Michael's C of E High School.

Name:	
Date:	
Signature:	

Appendix 4: Social Media etiquette guide. A guide for staff posting on the school Social Media account.

What Social Media does the school use:

The school uses Instagram, Facebook and X (formerly Twitter) to communicate thoughts and ideas within a set number of characters and usually references people, places and activities that tend to invite replies including photos. Social Media accounts can follow other Social Media accounts or be followed by other Social Media accounts and all comments are public. Users can Direct Message (DM) other users should they wish something not to be made for public viewing.

Why will staff at St Michael's be using the school Social Media accounts?

We will be using school Social Media to share and showcase all the fantastic things that happen at our Christian school and give an insight into life in all its fullness here at St Michael's.

Staff are asked not to use the school Social Media account to engage with parents directly, and that all communications are sent as overall announcements and notices to all our Social Media community.

Before sharing content on the school Social Media accounts, all staff should make sure they have read the St Michael's Social Media etiquette guide and follow this guidance.

Social Media etiquette guide:

- Any comments from the official school accounts will be grammatically correct and will not contain text or slang language
- No comments will ever contain offensive language, comments that undermine or abuse aimed at the school, its staff, parents/carers, governors, or any other persons that are affiliated with our wider school community
- Comments may contain hashtags to associate a comment with the related Social Media account e.g., #TeamSaintMichael's
- To safeguard our pupils, please ensure that no pupils surnames are listed below pictures
- Ensure that we have photographic consent of all pupils before posting pictures on Social Media
- Do not make any changes to the schools Social Media account settings and any issues should be reported to the ICT technicians by logging a ICT Helpdesk ticket on Synergy
- Social Media will be thoroughly monitored to ensure that we are not following any persons that are unsuitable or not adding value to our school
- Make sure to check images and text for copyright before posting
- Do not share the school Social Media log in details with anybody outside of school
- Ensure to read the Social Media checklist before sending any comments
- Ensure to keep up to date with online safety policy
- Please do not follow the schools Social Media account with your personal Social Media accounts
- You should not direct message people on the school Social Media accounts, any communications with outside agencies/persons should be done so via a school email account. Thus keeping communications professional and fostering a positive brand image

Inappropriate use, for example using Social Media to target others, will result in the Head teacher and Governing Body being informed, the member of staff involved will be dealt with according to the relevant disciplinary procedure.

Social Media checklist:

Do:

- Do use good professional levels of language and content. All information posed should be in a formal, courteous, and professional tone
- Do refer to the email etiquette guide appendix 1
- Do ensure no information written would bring the schools' reputation into disrepute
- Do ensure to proofread all comments before posting
- Do post comments at a reasonable time during working hours
- Do post comments that contain photos and quotes of our school life to showcase our school and engage our wider school audience
- Do ensure that we have photographic consent of all pupils before posting pictures on Social Media
- Do use email, not Social Media to ask a question requiring a long answer or to contact people
- Do remember it is not usually useful nor appreciated if you put someone's Social Media username in a post to get them to notice you (email the user instead)
- Do make use of hashtags. On Social Media you can use a hashtag at the end of a comment to enable these comments to be part of other related comments e.g., #TeamSaintMichaels
- Do try to showcase your department's talents by commenting at least every half term

Do not:

- Do not post any comments from the official school account will be grammatically correct and will not contain text or slang language
- Do not use offensive words of any description are forbidden
- All communications shall comply with good equal opportunities and non-discriminatory practices
- Do not post any information that would bring the schools' reputation into disrepute
- Do not follow the school Social Meida account from your personal accounts
- Do not post any content or photos of pupils without checking consent
- Do not make any changes to the school Social Meida account settings and any issues should be reported to the ICT technicians by logging a ICT Helpdesk ticket on Synergy
- Do not post any content that may contain copyright e.g., text or images that are not our own
- Do not share the school Social Meida log in details with anybody outside of school
- Do not private direct message people on the school Social Meida accounts, any communications with outside agencies/persons should be done so via a school email account

Appendix 5: Using Microsoft Teams

Any digital communication between staff and pupils or parents / carers (email, chat, VLE, Teams etc) must be professional in tone and content. These communications should only take place on official school systems.
Microsoft Teams may be used in school to communicate with classes, set home learning tasks and to facilitate live lessons as part of our remote learning offer. Staff at St Michael's may also use Microsoft Teams to contact pupils whom, for various reasons are unable to attend school.

- All members of Team St Michael's should access Microsoft Teams using their school email address
- Promote 'excellent behaviour' on Teams as in the classroom
- All Teams should only be set up and managed by the ICT technical support staff
- Staff should not be in a team with only one pupil
- Teachers must use professional language on Teams and moderate comments made by pupils
- Staff and pupils should only be added to appropriate teams. They should raise concerns to their line manager or teacher should they feel they have been added to a team by mistake
- Where meetings are used for online lessons, teachers should ensure that meeting settings are appropriate, including using a 'lobby' to admit pupils and restricting who can present
- Where possible, it is recommended that meetings (including live lessons) are scheduled in advance (this allows pupils to see lessons in their own Outlook calendar)
- When attending virtual meetings or live lessons, staff must ensure they wear professional and appropriate attire and use a nondescript background or use the Teams background blur setting
- Screen sharing can be used to share lesson resources and PowerPoints, however where possible, refrain from sharing the desktop and sensitive information
- Safeguarding concerns should be raised to the DSL using the usual safeguarding procedure
- Staff should keep a record of attendance for live lessons

Appendix 6: Recommendations for staff social media accounts

We acknowledge the benefits of social media for all members of Team St Michael's however, there are risks related to social media for staff to be aware of. Below are recommendations for staff to keep their data protected, particularly when using social media.

- Ensure privacy settings on all social media accounts are adequate to determine who can view posts and photographs
- Ensure visible profile picture is appropriate
- Consider using an alternative name on social media so that you cannot be found as easily e.g. first and middle name or alternative spelling
- Do not post anything that construed as defamatory or discriminatory against others (this may be writing on posts, pictures, or groups)
- Do not befriend pupils or parents on any form of social media
- Remember that reposting or retweeting can be viewed as a sign of endorsement (this may be inappropriate in some circumstances)
- Review posts from many years ago to see if these are appropriate
- When joining or being added to groups (for example Facebook groups), check whether it is Public, Closed (where anyone can see the members of the group but not the discussion) or Secret (where neither the members or the discussion are visible)