SSMJ POLICY FOR

Online Safety

Following the example of Jesus, together we learn, love and respect one another to be the best we can be.

Written by: Z Mabbott

Role: Headteacher

Date policy agreed: September 2025

Date to be reviewed: September 2027 or as required

Policy Overview:
The purpose of this policy is to safeguard and protect all members of St Michael & St John's online community by providing a framework to promote and maintain a safe, effective and responsive online safety culture. The policy is applicable to all members of St Michael & St John's. This includes staff, students and pupils, volunteers, parents/carers, visitors and community users who have access to and are users of St Michael & St John's digital technology systems, both internally and externally.

References:
Department for Education (DfE) (2025) Keeping Children Safe in Education: statutory guidance for schools and colleges. London: DfE.
Department for Education (DfE) (Jan 2023) Teaching online safety in schools.
https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teachingonline-safety-in-schools
Department for Education (DfE) (2023) Working together to safeguard children. London: DfE
Department for Education (2014) Cyberbullying: Advice for headteachers and school staff. London: DfE.
Children Act 1989
Children Act 2004
Communications Act 2003
Computer Misuse Act 1990
Criminal Justice and Courts Act 2015
Data Protection Act 1998
Data Protection Act 2018
Data (Use and Access) Act 2025
Education Act 2011
Education and Inspections Act 2006
Freedom of Information Act 2000
General Data Protection Regulations (2018)
Malicious Communications Act 1988
Prevent Duty Guidance 2023
Serious Crime Act 2015
The Lancashire ICT Security Framework (2005)
United Kingdom Council for Child Internet Safety (UKCCIS) Education for a connected world framework (2020)

Voyeurism (Offences) Act 2019

This policy links with other policies and practices

- ***Whistleblowing***
- ***Anti-bullying***
- ***Acceptable Use Policies (AUP)***
- ***Behaviour policy***
- ***Safeguarding policy***
- ***Code of conduct***
- ***Complaints policy***
- ***Confidentiality and data protection policy***
- ***Curriculum policies***
- ***Mobile Phone policy***
- ***Social Media policy***
- ***Staff handbook***

Disclaimer

Every effort has been made to ensure that the information contained within this policy is up to date and accurate and reflective of the latest legislative and statutory guidance. If errors are brought to our attention, we will correct them as soon as is practicable.

CONTENTS

1. **Introduction**
2. **Online Safety School Statement**
3. **Policy Scope**
4. **Security and data management**
5. **Roles and Responsibilities**
6. **Education and Training**
7. **Use of mobile phones**
8. **Digital media**
9. **Communications technology**
10. **Infrastructure and technology**
11. **Learners**
12. **Cultivating a Safe Environment**
13. **Online behaviour**
14. **Responding to Online Safety Concerns**
15. **Online Radicalisation and the Prevent Duty**
16. **Responding to Complaints**
17. **Monitoring and Compliance**
18. **Development of the Policy**
19. **Appendices**

1. Introduction

At St Michael and St John's School, Online safety is of paramount importance. In the current climate computing and networking through the use of online resources is instrumental in education. As the online world evolves, so do both the online harms and risks facing our children and the relevant legislation, both statutory and non-statutory, which directs and guides how schools should meet their online safety requirements.

School staff and governors play a vital role in setting an example for the whole school and are central to implementing policy and process. It is imperative that a whole school community approach to online safety is adopted and that all stakeholders are aware of their responsibilities and duties in relation to keeping children safe online. This will support a robust online safety ethos and ensure that schools are providing the best online safety provision they possibly can.

This policy is applicable to all members of St Michael & St John's. This includes, staff, students and pupils, volunteers, parents/carers, visitors and community users who have access to and are users of the St Michael & St John's digital technology systems, both internally and externally within the home and community setting.

Online Safety will naturally tend to focus on reducing the potential risks; however, it should equally promote the benefits to be gained from the opportunities afforded through the use of technology.

Review of the Policy

This Online Safety Policy has been reviewed by the Head Teacher and shared with the:

- Online Safety Lead,
- Staff,
- Governors,
- Parents and carers,
- Children

Key people / Dates

The implementation of this Online Safety Policy will be monitored by the:	*Zoe Mabbott (Headteacher and DSL)* *Marc Duckworth (Deputy DSL and Online Safety Lead)* *Olivia Whyman ((Deputy DSL)*
Network Manager / other technical support	*John Kavanagh and Patrick Costelloe*
Monitoring will take place:	*Termly*
The Online Safety Policy will be reviewed annually, or more regularly in light of any significant new developments in the use of technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*September 26*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LA safeguarding officer, LADO, CSC, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents (CPOMS),
- Monitoring logs of internal activity,
- Surveys/questionnaires:
- Pupil,
- Parents/carers,
- Staff

2. Online Safety School Statement

St Michael & St John's School asserts that online safety is an essential element of safeguarding and duly acknowledges its statutory obligation to ensure that all learners and staff are protected from potential online harm.

At St Michael & St. John's Roman Catholic Primary School we aim to secure the best for all pupils as individuals. We strive for them to be the best that they can be.

'The heart of the discerning acquires knowledge, for the ears of the wise seek it out.' Proverbs 18:15

This approach means that every effort is made to promote a positive school climate that recognises the rights of all pupils. These rights include the right to stay safe at all times, including when using technology both in school and out. Online Safety is at the heart of all our teachings in order to enable and encourage all those involved with school to have a safer use of technology.

We aim to provide a diverse, balanced and relevant approach to the use of technology. The children are encouraged to maximise the benefits and opportunities that technology has to offer in a safe and enabling environment. St Michael & St John's School believes that the internet and associated devices are an integral part of everyday life.

St Michael and St John's school ensures that children learn in an environment where security measures are balanced appropriately with the need to learn effectively, whilst also equipping the children with the skills and knowledge to use technology appropriately and responsibly.

We teach how to recognise the risks associated with technology and how to deal with them, both within school and outside the school environment. The school affirms that all learners should be empowered to build resilience and to develop strategies to recognise and respond to online risks. All users in the school community understand the need for an Online Safety policy.

3. Policy Scope

Online safety is an omnipresent topic which requires recurrent regulatory review and places a stringent duty of care on us all. This policy supports school in meeting statutory requirements as per the DfE guidance under KCSiE (2025), Working together to safeguard children (Dec 23) and non-statutory guidance, Teaching online safety in schools (2023). Effective, timely and robust online safety is fundamental to protecting children and young people in education and it is a significant part of the safeguarding agenda.

High quality online safety provision requires constant vigilance and a readiness to act where abuse, exploitation or neglect is suspected. The landscape of safeguarding is constantly evolving, and educational establishments must endeavour to embrace and shape their key priorities in support of this. Education has a vital role to fulfil in protecting children and young people from forms of online abuse whilst demonstrating a concerted obligation to respond with haste and flexibility to concerns as they arise. Above all, all staff must foster dedication to ensuring that they listen to the voices of the vulnerable and act upon what is heard. Safeguarding is everyone's responsibility.

Defining online abuse NSPCC – Online abuse is any type of abuse that happens on the internet. It can happen across any device that's connected to the web, like computers, tablets and mobile phones. And it can happen anywhere online, including:

- social media
- text messages and messaging apps
- emails
- online chats
- online gaming
- live-streaming sites.

Types of online abuse may include:

- Cyberbullying
- Emotional abuse
- Grooming
- Sexting
- Sexual abuse
- Sexual exploitation

The types, patterns and different circumstances of significant harm and abuse should be considered within the categories identified for children in the Children Act 1989 / 2004. These are:

- Neglect
- Sexual
- Physical
- Emotional

Technology can facilitate a world of learning and development in addition to help yield a range of opportunities. However, the stark reality is that it can also present a window to potential and actual harm and abuse. It can elicit and support an array of illegal abusive behaviours including, but not limited to:

- Harassment
- Stalking
- Threatening behaviour
- Creating or sharing child sexual abuse material
- Inciting a child to sexual activity
- Sexual exploitation
- Grooming
- Sexual communication with a child
- Causing a child to view images or watch videos of a sexual act.

This policy should be read alongside the relevant policies relating to safeguarding of children and in addition to the associated statutory legislation and guidance as stipulated on pages 2 and 3 of this policy.

4. Security and data management

ICT security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment. The *Lancashire ICT Security Framework* been consulted to ensure that procedures are in place to ensure data, in its many forms, is kept secure within the school.

In line with the requirements of the General Data Protection Regulations (2018), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data is:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection.

All data in our school is kept secure and staff informed of what they can or can't do with data through the online safety Policy and statements in the Acceptable Use Policy (AUP). See Appendices 1- 4

The school bursar, under direction from the Headteacher, has the responsibility for managing information and allows staff some access to personal data whilst showing understanding of their legal responsibilities.

St Michael & St John's school ensures that data is appropriately managed both within and outside the school environment as all staff, Governors, supply teachers etc. adhere to the Acceptable Use Policy relevant to them. Also, the above named groups use secure email for contact regarding school matters, these emails are managed by Lancashire Local Authority and are treated with confidence ensuring no confidential information can be accessed. Staff are aware that they should only use approved means to access, store and dispose of confidential data. Staff are aware of the dangers of unsecured wireless access at home when accessing school data remotely. In line with GDPR (General Data Protection Regulation) Children's profiles, names and/or information pertaining to the school are not stored using 'cloud' storage facilities e.g. Dropbox/ SkyDrive.

Teachers are provided with a school laptop (mobile device), these are password protected and confidential information is stored securely on these. Personal devices are not used to access data on school systems e.g. downloading e-mail or files. The school back up all data on the Bursar's system at the end of every day to ensure the risk of data lost is addressed and managed.

Data is backed up on the bursar's system every night and this information is stored securely in accordance with recommended guidance from Lancashire Local Authority.

5. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of all stakeholders across the online community within St Michael & St John's School:

5.1 Teachers and Staff

All members of school staff (teaching and non-teaching) have a responsibility to protect children online. This includes every member of staff who works at the school; Headteacher, teachers, teaching assistants, substitute teachers, work-experience staff, office staff, welfare staff, caretakers, cleaners, etc. All teachers and staff must always act in accordance with their own professional boundaries, upholding professional behaviour and conduct at all times.

All school staff need to:

- Have an up to date awareness of online safety matters and the current online safety practices of the school.
- Be aware of and adhere to all policies in school which support online safety and safeguarding.
- Contribute to policy development and review.
- Support in the ownership and responsibility for the security of systems and the data accessed.
- Model good practice when using technology.
- Know the process for making referrals and reporting concerns.
- Know how to recognise, respond and report signs of online abuse and harm.
- Receive appropriate child protection training.
- Always act in the best interests of the child.
- Be responsible for their own continuing professional development in online safety.

5.2 Governors and Senior Leadership Team

A governor's role for online safety in a school should include, but is not limited to:

- Upholding online safety as a safeguarding issue which is embedded across the whole school culture.
- Ensuring that children are provided with a safe environment in which to learn and develop.
- Ensuring that the school has appropriate filters and monitoring systems in place.
- Ensuring the school has effective policies and training in place.
- Carrying out risk assessments on effectiveness of filtering systems.
- Auditing and evaluating online safety practice.
- Ensuring there are robust reporting channels.

5.3 Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Leads (Deputy DSL)

With respect to online safety, it is the responsibility of the DSL to:

- Ensure children and young people are being appropriately taught about and know how to use the internet responsibly.
- Ensure teachers and parents are aware of measures to keep children safe online through relevant training provision.
- Take responsibility for all safeguarding matters, including online safety.
- Collaborate with the senior leadership team, the online safety lead and computing lead.
- Facilitate effective record keeping and the reporting and monitoring of all online safety concerns.
- Promote online safety and the adoption of a whole school approach.
- Maintain own training and learning needs, ensuring they are up to date with all matters relating to online safety.

5.4 IT Provider

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL or Online Safety Lead for investigation and action

5.5 Children and Young People

With respect to online safety in your school, children need to:

- Know who the DSL is.
- Engage in age appropriate online safety education opportunities.
- Contribute to policy development and review.
- Read and adhere to online safety policies.
- Respect the feelings of others, both off and online.
- Take responsibility for keeping themselves and others safe online.
- Where and how to find help with any online incidents or concerns.
- How, when and where to report concerns and when to seek help from a trusted adult.

The UKCCIS 'Education for a Connected World' framework aims to equip children and young people for digital life. It covers:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing and lifestyle
- Privacy and security
- Copyright and ownership

5.6 Parents and Carers

Parents and carers need to understand the risks that children face online to protect them from online dangers. Parents need to:

- Read and adhere to all relevant policies.
- Be responsible when taking photos/using technology at school events.
- Know who the school DSL is.
- Know how to report online issues.
- Support online safety approaches and education provision.
- Be a role model for safe and appropriate behaviour.
- Identify changes in children's behaviour that could indicate they are at risk of online harm or abuse.

6. Education and Training

Safeguarding activity across the United Kingdom (UK) continues to intensify in volume and intricacy with national influences relating to political uncertainty, a rise in poverty, an increase in the ageing population, sustained funding pressures and increased demand for child and adult services.

Furthermore, a commitment to ensuring the provision of an integrated and highly robust safeguarding service for all ages is essential. Effective online safety provision and promotion of the welfare of children and young people relies upon constructive relationships that are conducive to robust multi-agency partnership working. This can only be effective when all staff are knowledgeable, confident and equipped with the skills to deal with processes and procedures when concerns arise relating to online abuse or harm.

Online safety has a high emphasis on a competent well-established workforce, up to date policies and procedures, robust governance arrangements and collaborative practices. Types of online risk usually fall under one of four categories:

Contact: Contact from someone online who may wish to bully or abuse the child. This could also include online grooming, online harassment or activities of a commercial nature, including tracking and harvesting person information.

Content: Inappropriate material available to children online including: adverts, spam, sponsorship, personal info, violent or hateful content, pornographic or unwelcome sexual content, biased materials, racist materials, and misleading information or advice.

Conduct: The child may be the perpetrator of activities including: illegal downloading, hacking, bullying or harassing another child. They might create and upload inappropriate material or provide misleading information or advice.

Commerce: This includes online gambling, inappropriate advertising, phishing or financial scams.

7. Use of mobile devices

School use of mobile devices, including laptops, tablets, mobile phones, cameras and games consoles is becoming more commonplace. Whilst these can provide a flexible solution and offer a range of exciting opportunities to extend children's learning, their use poses challenges in terms of online safety. Many of these devices integrate functionality to take images, access the Internet and engage users in various methods of external communication.

St Michael & St John's school provides some devices e.g. iPads for use in class but do not allow staff (or children) to bring personal devices into school to use as resources for teaching and learning,

Our school has considered what is acceptable with regard to the use of mobile phones and cameras. This is that staff do not use their personal mobile devices (including phones) when the children are within the environment, they are to be used (unless specific permission has been given by the Headteacher) during breaks or lunch or out of lesson times. In the event that a personal mobile device needs to be accessed during the school day this should be done so in a room/ environment where children are not present. These personal devices should not be used for photographs or storage of school data. In response to the requirements of the EYFS framework, and to avoid confusion or misinterpretation, our school has implemented procedures with respect to mobile devices across the whole school.

7.1 Mobile phones

Mobile phones can present a variety of challenges if not used appropriately and we have definite and clear boundaries for their use. They are valuable items that can be lost, stolen or damaged in the school environment and could also be considered as distracting or intrusive in a teaching or learning situation. However, staff and parents may equally have valid reasons why mobile phones should be readily available. Rules for mobile phone use are (including those mentioned above) children needing a mobile phone for walking to/ from school (with permission from parents) should hand it to the class teacher for safe keeping until the end of the school day, a signed letter needs to be sent by parents giving permission for the child to have the phone in school. At the end of the school day, the mobile phone will be returned to the child and must not be switched on until the child has exited the school premises. Staff mobile phones should be on silent during the school day. Staff and visitors can be contacted in the event of emergency via the school office. Images, video or audio must not be recorded on a personal mobile phone without specific authorisation from the Headteacher.

Users are allowed to access the Internet via personal mobile phones (during their own time) using the school's secure wi- fi connection after getting the password from the school office. There is a 'work' device for staff to use, for example, whilst outside the main buildings or on trips, the use of this is subject to the Acceptable Use Policy and should be used in an emergency situation. School data, photos, video/ audio should not be stored on this device. It is the responsibility of the last person to use the device to ensure it is always ready for use e.g. fully charged and 'in credit' (the school bursar needs informing regarding 'credit'). Visitors, including parents are made aware of our rules for acceptable use of a mobile phone through the publication of the online safety policy on the school website.

Staff are aware of the potential for mobile phones to be used for cyberbullying through training and anti-bullying activities during anti-bullying week in November of each year as well as online safety week activities each February. Cyberbullying prevention activities are completed during these two designated weeks in November and February. The reporting of cyberbullying is to be done through the Headteacher/ Deputy DSL who will then follow these steps;

- Ask the child not to reply
- Save the evidence
- Block the bullies
- Explain the severity to the bully
- Contact parents of involved parties
- Inform the website involved e.g. Facebook, twitter or Youtube
- Get advice from Lancashire Local Authority
- Contact police where applicable

7.2 Other mobile devices

The school allows use of personal mobile devices during their own time in school by adults in line with the Acceptable Use Policy (Appendices 1-4). The adult is allowed access to the internet using the school's secure wi- fi connection after getting the password from the school office; this will then mean the mobile device is subject to the same filters as school devices. The device owners will be aware of their responsibility to ensure all content on these devices is legal and appropriate for a school setting through the Acceptable Use Policy. The owners are also aware that the school cannot be held liable e.g. for any damage or theft of personal devices. Devices should be 'virus checked' (if applicable) before use on school systems by the owner.

Physical security of school based devices is through the devices being locked away at night, classrooms are locked when applicable as well as the school monitored alarm system being in use.

7.3 Tablet devices:

Copyright legislation is compliant when purchasing content through discussion with computer technician and/or advice from content suppliers. Content is transferred between devices under direction of the technician and via the use of 'cloud' storage linked to secure email accounts provided by Lancashire Local Authority. Users are aware of any 'sanctions' for misuse of mobile devices through the Acceptable Use Policy.

8. Use of digital media (cameras and recording devices)

Photographs and videos of children and adults may be considered as personal data in terms of The Data Protection Act (2018). To ensure all users are informed about the risks surrounding taking, using, sharing, publishing and distributing digital media, we have decided on the following points for inclusion in our Online Safety Policy.

8.1 Consent and Purpose

Written consent from parents for photographs of their children to be taken or used is covered through the image consent form in the appendices (6-8). When consent is gained it is made clear how photographs can/ cannot be used (including the use of external photographers or involvement of 3rd parties.)

The consent includes permission to store / use images once a child has left the school e.g. for brochures, displays etc. with parents being informed of the timescale for which images will be retained. This permission is obtained annually and parents are requested to inform the school of any change in circumstances that may necessitate removal of permission, enabling the Headteacher/ Deputy DSL to action removal of images.

Parents are informed of the purposes for which images may be taken and used e.g. displays, website, brochures, learning journeys and portfolios, press / other external media through the image consent form.

Some images are displayed in public areas e.g. the entrance hall and office area, with the purpose of these being the different roles and responsibilities of the children e.g. digital leaders, sports clubs, school council members, the GIFT team etc. and children volunteer/ are elected for these roles.

The consent form covers the use of children's images to be included in portfolios maintained by trainees / students not directly employed by the setting; the form also covers the use of images in group situations such as those used in children's profiles in the EYFS setting. Due to the image consent form being updated annually this ensures only current images are used, i.e. not children / adults who have left the setting.

The press has special permissions in terms of Data Protection and may wish to name individual children to accompany a photograph and at times, the media may publish an image in their online publication which may offer facilities for the 'public' to add comments in relation to a story or image. These can potentially invite negative as well as positive comments. These are explained to parents on the image consent form, and any names will be first names only unless specified otherwise (in which case specific permission must be sought).

All adults working in the setting are kept informed of any children / other adults whose photographs must not be taken through details being kept in a list by the bursar, and adults must request this information prior to taking/ using images of children/ adults.

8.2 Taking Photographs / Video

All staff are authorised to take images as long as they have signed the AUP which states that any images/ videos taken should only be using school equipment unless specific permission is given by the Headteacher. When taking photographs/ video the rights of an individual to refuse to be photographed is respected and it is ensured that the photograph doesn't show children who are distressed, injured or in context that could be embarrassing or misinterpreted. Every effort is made to ensure certain children are not continually favoured when taking images. Subjects are appropriately dressed and not participating in activities that could be misinterpreted including when considering the angle of shots for children engaged in P.E. activities. Certain areas are classed as 'off limits' for taking photographs, e.g. toilets, cubicles etc. Close up shots are avoided as these may be considered intrusive. Shots should preferably include a background context and show children in group situations.

8.3 Parents Taking Photographs / Videos

Under the Data Protection Act (2018), parents are entitled to take photographs of *their own* children on the provision that the images are for *their own* use, e.g. at a school production. Including other children or other purpose could constitute a potential breach of Data Protection legislation. Through the image consent form parents are informed that they should only take photographs/ videos of their own children (special events such as performances are covered separately using the 'consent form for images at a special event') parents are reminded of this at the beginning of each year when signing the consent form and the special event form (Appendix 7).

8.4 Storage of Photographs / Video

Images are stored securely on the school computers and are not stored on portable devices, USB memory sticks or in 'cloud' storage. We do not allow images to be stored outside of the school equipment unless it is stored by the school photography company and is in line with the Data Protection Act (2018). Staff are not allowed to store images on personal equipment e.g. tablets, laptops or USB storage devices. Only staff have access to images and videos stored on school equipment due to the images being stored in staff only, password protected domains.

It is the responsibility of all teachers, the Headteacher/ Deputy DSL for deleting photographs / video or disposing printed copies (e.g. by shredding) once the purpose for the image has lapsed or should a parent withdraw permission. If photographs are 'sent' electronically, this is done using the school staff allocated emails which are hosted by Lancashire local authority.

8.5 Publication of photographs/ videos

Publication of images is only done through the secure school website which is hosted by Lancashire local authority and the images are of children whose parents have given permission using the image consent form (Appendices 6-7).

When publishing photographs, care is taken over the choice of images to ensure that individual children / adults cannot be identified or their image made available for downloading or misuse, e.g. through the use of low definition images that will not magnify effectively. Full names and/ or other personal information does not accompany published images.

8.6 When publishing images

Staff are aware that full names and personal details will not be used on any digital media, particularly in association with photographs. They also recognise the risks associated with publishing images, particularly in relation to use of personal Social Network sites. Children's images may only be shared on the school's Dojo, Twitter or Facebook pages (with parental permission). It is also recognised that staff ensure their personal profiles are secured and do not display content that is detrimental to their own professional status or could bring the school into disrepute.

8.7 The media, 3rd parties and copyright

3rd parties are supervised whilst in the school and are able to comply with the Data Protection requirements in terms of taking, storage and transfer of images. The school owns the copyright for images taken by a 3rd party. If uploading images to a 3rd party website, e.g. for printing or creating calendars, cards etc. it is ensured that the person uploading reads the terms and conditions of the website. Permission could unknowingly be granted for the site's host license to modify, copy or redistribute images without further consent. The site may also be advertised for 'personal use' only therefore using for business purposes would be a breach of the terms and conditions.

8.8 CCTV, video conferencing, VOIP and webcams

St Michael and St John's RC Primary School does not use CCTV, video conferencing, VOIP or webcams, however, Zoom can be used by children (with peers), when at home, to attend scheduled meetings with staff (see risk assessment).

9. Communications technologies

School use a variety of communication technologies and need to be aware of the benefits and associated risks. New technologies are risk assessed against the potential benefits to learning and teaching before being employed throughout the school. This is done before multiple devices are purchased. As new technologies are introduced, the online safety Policy is updated and all users are made aware of the changes.

9.1 E-Mail

The following statements reflect good practice in the use of email;

- All users have an Office365 email which any school information is sent via; these are the recommended email by Lancashire.
- Staff have permission to access personal email accounts on school equipment provided it is in accordance with the AUP (in appendix).
- The junior children have email accounts which have been set up using the Office365 service and these have been set in such a way that the children cannot be identified by them e.g. j.smith@ssmj.lancs.sch.uk
- Staff and children are made aware that only official email addresses should be used for contact.
- The Lancashire Grid for learning filtering service should reduce the amount of SPAM (junk mail) received on school email accounts.
- All users are aware of the risks involved in accessing content including SPAM, phishing, unsuitable materials and viruses from external email accounts e.g. Hotmail or Gmail in school.
- All users are aware that the email is covered by the Data Protection Act (2018) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users are aware that email may be monitored at any time in accordance with the Acceptable Use Policy.
- The content of children's email accounts is monitored by the class teachers, Headteacher/ Deputy DSL and parents of each child.
- Users should report any content that makes them feel uncomfortable, is offensive, threatening or bullying in any way to the online safety champion.
- Users are aware they should not open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal act.

9.2 Social Network sites

Social Network sites allow users to be part of a virtual community. Current popular examples of these sites are Facebook, X, Instagram, Snapchat and Tik Tok, also some interactive computers such as Xbox and Switch. These sites provide users with simple tools to create a profile or page including basic information about themselves, photographs, and possibly a blog or comments. As a user on a Social Network site, you may have access to view other users' content, send messages and leave unmediated comments. Many Social Network sites are blocked by default through filtering systems used in school.

Although use of Social Network tends towards a personal basis outside of school environment, their use as a tool for communicating with parents is becoming more commonplace in primary schools. St Michael and St John's School uses Facebook, X and class dojo. Guidance for personal publishing sites is included as part of staff induction, discussed regularly and outlined in the staff Acceptable Use Policy – along with sanctions for inappropriate use.

Whatever methods of communication are used, individuals should always conduct themselves in a professional manner. If content is made available on the web it is available for everyone to see and potentially remains there forever. Please also refer to the school's social media policy.

All staff are aware of the following points:

- The content on Social Network sites may be unmediated and inappropriate for certain audiences.
- If a Social Network site is used personally, details must not be shared with children and privacy settings be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.
- They must not give personal contact details to pupils or parents/ carers including mobile telephone numbers, details of any blogs or personal websites.
- The content posted online should not:
  - bring the school into disrepute
  - lead to valid parental complaints
  - be deemed as derogatory towards the school and/ or its employees
  - be deemed as derogatory towards pupils and/or parents and carers
  - bring into question their appropriateness to work with children and young people.
- Adults must not communicate with children using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted. Online Communications with parents, past pupils or siblings of pupils, especially if under the age of 18 should be discouraged. If a child emails a teacher with homework etc. using the child's personal email account, their parent must be copied in to any reply given.
- Children must not be added as 'friends' on any Social Network sit. It is recommended that parents are also not added as 'friends' (see social media policy).

The school has also considered the advice provided for parents in terms of their use of Social Networking sites and how the school will respond to identified issues. Common concerns that have had consideration include:

- Posting inappropriate comments about staff or children that could be construed as instances of cyberbullying.
- Posting of images of children or adults on profiles without permission of the individuals involved, especially if the photographs contain children other than their own.

9.3 Websites and other online publications

Information posted online is readily available for anyone to see and thus form an opinion about the school. From September 2012, the School Information (England) (Amendment) Regulations 2012 specified that certain, up to date information must be made available on a school's website.

At St Michael and St John's RC Primary school we ensure that:

- The school website is effective in communicating online safety messages to parents and carers as this policy is on the school website and there are also links to useful online safety websites.
- Everybody in the school is made aware of the guidance for the use of digital media on the website/ online publication.
- Everybody in the school is aware of the guidance regarding the inclusion of personal information on the website/ online publication.
- Staff have limited access to edit online publications and ensure the content is relevant and current with the Headteacher, web editor and web host having overall responsibility for what appears on the website.
- There is no content that needs to be hidden behind a password protected area.
- Downloadable materials are in a read-only format (PDF) where necessary, to prevent content being manipulated and potentially redistributed without the school's consent.

9.4 Artificial Intelligence (AI) systems in school

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools:

- learner support
- teacher support
- school operations

At St Michael and St John's, ensuring all of the above use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role. The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

In regards to AI, the school will:

- comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR
- protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose.
- provide relevant training for staff and governors in the advantages, use of and potential risks of AI.
- support staff in identifying training and development needs to enable relevant opportunities.
- seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works; its potential benefits, risks, and ethical and social impacts.
- ensure AI tools used comply with UK GDPR and other data protection regulations and verify that tools meet data security standards before using them for work related to the school.
- ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs.
- report any incidents involving AI misuse, data breaches, or inappropriate AI outputs immediately to the headteacher or Deputy DSL.
- audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, documenting all tools in use, their purpose and potential risks.

10. Infrastructure and technology

The school ensures that the infrastructure/ network is as safe and secure as possible. The school subscribe to the Lancashire Grid for learning/ CLEO Broadband Service, therefore the internet content filtering is provided by default. It is important that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. Sophos Anti-Virus software is included in the school's subscription and this is installed on computers in school and then configured to receive regular updates.

10.1 Children's access

The children are supervised when accessing school equipment and online materials (e.g. working with a trusted adult). The children have limited access to the school systems through class/ personal logins, this access is restricted to certain areas of the network. KS2 children all have personal log in details (with the same password for ease of access for teachers) and KS1/ EYFS children have a class log in. Children must never be allowed to access school computers/ internet unsupervised in school. (The computing lead teacher and Headteacher have access to all children's accounts via an icon when using a personal log on).

10.2 Adult access

Staff have logins where most of the school systems are available to them, with the others have a hierarchical level of access increasing in the order shown - head and ICT technician (who have full access) and ICT coordinator.

10.3 Passwords

All staff are aware of the guidelines in the Lancashire ICT Security Framework for Schools. All users of the school network have a secure username and password. The administrator password for the school network is available for the Headteacher and ICT Coordinator and is kept in a safe place. Staff and children are reminded of the importance of keeping passwords secure.

10.4 Software/ hardware

School have legal ownership of all software (including apps on tablet devices), and an up to date record of appropriate licenses for all software is kept. The Bursar, ICT Coordinator and ICT Technician are responsible for maintaining this. School regularly audit equipment and software with installation of the software being under control of the Headteacher and technician.

10.5 Managing the network and technical support

Servers, wireless systems and cabling are securely located and physical access is restricted. All wireless devices have security enabled and these devices are only accessible through a secure password available from the school bursar. Relevant access settings have been restricted on tablet devices e.g. downloading of apps or 'inapp' purchases. The Headteacher and ICT technician are responsible for managing the security of the school network through regular visits from the technician enabling him to update the system with critical software updates/ patches.

Users (staff, children and guests) have clearly defined access rights to the school network through the usernames and passwords, with permissions assigned by the Headteacher and ICT Coordinator. Staff and children are reminded to lock or log out of a school system when the computer/ digital device is left unattended. Users are not allowed to download executable files or install software. The Headteacher and ICT technician have responsibility for assessing and installing new software. Users report any suspicion or evidence of a breach of security to the Headteacher/ Deputy DSL.

The school's guidance on using removable storage devices on school equipment is that children must seek permission from their teacher before being allowed to use these devices and staff can use them in accordance with the Acceptable Use Policy. Network monitoring takes place in accordance with the Data Protection Act (2018). All internal/ external technical support providers are aware of the school's requirements/ standards regarding online safety. The ICT Coordinator and Headteacher are responsible for liaising with / managing the technical support staff.

10.6 Filtering and virus protection

The school filtering is managed by Lancashire Grid for learning filtering (Netsweeper) service. Procedures are in place to ensure that ALL equipment including school laptops used at home are regularly updated with the most recent version of virus protection software used in school as these updates are completed automatically every time the internet is accessed, as recommended by KCSiE (2025).

11. Learners

St Michael & St John's school will promote safe and responsible internet use:

- Education regarding safe and responsible use and access of the internet.
- Include online safety in Personal, Social, Health and Economic (PSHE) education, Relationships and Sex Education (RSE) and Information Computer Technology studies.
- Reinforce online safety messages as a continuum.

SSMJ will support learner's understanding based on age and ability:

- Acceptable use posters in all rooms with internet access.
- Informing all learners of monitoring and filtering in place.
- Implement peer education strategies.
- Provide continuous training and education as part of their transition across key stages.
- Use alternative, complementary support where needed.
- Seeking learner voice. (Digital Leaders pupil group)

11.1 Vulnerable Learners

Vulnerable children who need our help the most are not only missing out on opportunities to flourish online, but are often experiencing the very worst that the online world can be. Over 2 million children in England are living in families with complex needs. Many children are living in families with domestic abuse, parental substance abuse and mental health problems.

St Michael & St John's School recognises that some learners are more vulnerable due to a range of factors. Those children may be:

- Receiving statutory care or support.
- Known to have experienced specific personal harm.
- With a disability, ill-health or developmental difficulties.
- In households or families with characteristics or locations that indicate higher potential likelihood of current and future harm.
- Vulnerable or of concern by virtue of their identity or nationality.
- At risk in relation to activity or institutions outside the home.
- Caring for others.

St Michael & St John's School will ensure the effective and safe provision of tailored online safety education, and will obtain input and advice from specialist staff as deemed necessary.

11.2 Staff

St Michael & St John's School will:

- Ensure provision of robust policies and practices as part of induction and ongoing training provision.
- Provide up to date online safety training at least annually or more in line with legislative and statutory changes and/or online safety incidents arising.
- Ensure training will include recognition of risks and responding to concerns.
- Inform of monitoring and filtering processes.
- Make staff aware that their online conduct outside of work can impact upon their professional role and responsibilities.
- Advise of appropriate resources.
- Ensure that all staff are aware of procedures to follow in recognising, responding and reporting online safety concerns.

11.3 Parents and carers

St Michael & St John's School will:

- Recognise and cultivate the essential role parents and carers have in fostering safer online safety practices in children and young people.
- Ensure provision of resources, support and advice.
- Ensure provision and adherence to online safety policies and other policies of relevance.
- Advise of how and when to raise concerns.
- Provide details of all relevant contacts (for example, the DSL).

12. <u>Cultivating a safe environment</u>

"All staff should be aware of indicators, which may signal that children are at risk from, or are involved with serious violent crime. These may include increased absence from school, a change in friendships or relationships with older individuals or groups, a significant decline in performance, signs of self-harm or a significant change in well-being, or signs of assault or unexplained injuries. Unexplained gifts or new possessions could also indicate that children have been approached by, or are involved with, individuals associated with criminal networks or gangs" (DfE, 2019).

Children should be educated in an age-appropriate way around:

- How to evaluate what they see online
- How to recognise techniques for persuasion
- Their online behaviour
- How to identify online risks
- How and when to seek support

12.1 Evaluate: How to evaluate what they see online

This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

St Michael & St John's School will help pupils to consider questions including:

- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?

- Why would someone want me to believe this?
- Can I trust what AI is telling me?

12.2 Recognise: How to recognise techniques used for persuasion

This will enable pupils to recognise the techniques that are often used to persuade or manipulate others. A strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

St Michael & St John's School will help pupils to recognise:

- Online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation).
- Techniques that companies use to persuade people to buy something.
- Ways in which games and social media companies try to keep users online longer (persuasive/sticky design)
- Criminal activities such as grooming.

13. Online Behaviour

This will enable pupils to understand what acceptable and unacceptable online behaviour looks like St Michael & St John's School will teach pupils that the same standard of behaviour and honesty applies online and offline, including the importance of respect for others. St Michael & St John's School will also teach pupils to recognise unacceptable behaviour in others.

St Michael & St John's School will help pupils to recognise acceptable and unacceptable behaviour by:

- Looking at why people behave differently online. For example, how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do.
- Looking at how online emotions can be intensified resulting in mob mentality.
- Teaching techniques (relevant on and offline) to defuse or calm arguments (for example, a disagreement with friends) and disengage from unwanted contact or content online.
- Considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

13.1 Inappropriate use

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 quickly and actions are proportionate to the offence. The school have decided what constitutes inappropriate use and the sanctions to be applied. Some examples of inappropriate incidents are listed below with suggested sanctions (also see appendix 12)

Incident	Procedure and sanctions
Accidental access to inappropriate materials.	Minimise the webpage/ turn off the monitor/ click the 'Hector Protector' button Tell a trusted adult Enter the details in the Incident log and report to 'Netsweeper' services if necessary Persistent 'accidental' offenders may need further disciplinary action.

Using other people's logins and passwords maliciously	• Inform Headteacher/Deputy DSL • Enter the details in the Incident log (and on CPOMs) • Additional awareness raising online safety issues and the AUP with individual child/ class • More serious or persistent offences may result in further disciplinary action in line with the behaviour policy • Consider parent/ carer involvement • If this is a member of staff, then the school discipline policy may be applicable.
Deliberate searching for inappropriate materials	
Bringing inappropriate electronic files from home	
Using chats and forums in an inappropriate way	

13.2 Identify: How to identity online risks

This will enable pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

St Michael & St John's School will help pupils to identify and manage risk by:

- Discussing the ways in which someone may put themselves at risk online.
- Discussing risks posed by another person's online behaviour.
- Discussing when risk taking can be positive and negative.
- Discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations; i.e. how past online behaviours could impact on their future when applying for a place at university or a job for example.
- Discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with.
- Asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

13.2 How and when to seek support

This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

St Michael & St John's School will help pupils by:

- Helping them to identify who trusted adults are.
- Looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations, such as Childline and the Internet Watch Foundation. This should link to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education).
- Helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

14. Responding to Online Safety Concerns

The safety of the child and young person is of paramount importance. Immediate action may be required to safeguard investigations and any other children and young people. Any concern that children and young people may be at risk of harm or abuse must immediately be reported. Reputational issues must be managed appropriately by discussion with the relevant communications team.

Online safety is recognised as part of the education settings safeguarding responsibilities – the DSL should take lead responsibility for online safety concerns which should be recorded and actioned. Children and young people will be enabled (at a level appropriate to their age and ability) to share online concerns. The child protection policy for St Michael & St John's School includes procedures to follow regarding online safety concerns.

Remember:

- Child welfare is of principal concern – the best interests of children take precedence.
- If there is any immediate danger, contact the police on 999.
- Refer to all appropriate agencies as per St Michael & St John's School local process.
- Always adhere to local safeguarding procedures and report to the DSL and Headteacher within Lancashire.

15. Online Radicalisation and the Prevent Duty

15.1 Scope and Commitment

SSMJ recognises that the internet provides access to a wealth of information, but it can also be exploited by extremists and terrorist groups to radicalise vulnerable individuals. In accordance with the statutory Prevent duty guidance, our organisation is committed to protecting individuals from the risks of extremist ideologies and radicalisation.

15.2 Staff Responsibilities and Training

All staff and volunteers must undergo appropriate Prevent and safeguarding training. Staff are required to be vigilant and aware of the signs of online radicalisation. This includes understanding how to recognise extremist content, changes in online behaviour, and vulnerabilities that make an individual susceptible to radicalisation.

15.3 Reporting Procedures

Any concerns regarding online radicalisation or extremism must be treated as a safeguarding concern and reported immediately to the Designated Safeguarding Lead (DSL). The DSL will assess the situation and, where necessary, escalate the concern to the local multi-agency safeguarding hub or the local police, following the national Prevent referral pathways.

15.4 Filtering and Monitoring

To minimise the risk of individuals accessing extremist material on our premises, we employ robust, age-appropriate filtering and monitoring systems on all network connections and devices. Access to known extremist websites and unapproved online communication channels are actively blocked.

15.5 Education and Awareness

We will proactively teach users about digital resilience, critical thinking, and potential dangers as part of our curriculum or safeguarding awareness sessions. Users will be taught how to report concerning content and how to manage their digital footprint safely

16. Responding to Complaints

There are a number of sources from which a complaint or allegation might arise, including those from:

- A child or young person
- An adult
- A parent/carer
- A member of the public (including a friend or relative)
- A colleague

There may be up to three components in the consideration of an allegation:

- A police investigation of a possible criminal offence.
- Enquiries and assessment by children's social care or adult social care relating to whether a child, young person or adult at risk is in need of protection or services.
- Consideration by an employer of disciplinary action in respect of the individual (including suspension).

It is also the responsibility of the member of staff to inform their line manager if they are being investigated in relation to children, young people or adults at risk with respect to protection concerns outside of work. They should also report if their own children/stepchildren/children they are living with become subject to child protection matters or an adult related to them or living with them become subject to adult protection matters. The line manager must report this to the DSL.

17. Monitoring and Compliance

Monitoring Requirements	For example: Analysing incident logs (CPOMS) Checking planning for online safety lessons Student, pupils, parents and carers questionnaires Evaluations Daily reports regarding web searches Filtering and monitoring reports.
Monitoring Prepared by	Headteacher/Deputy DSL/Online Safety Lead
Monitoring Presented to	Zoe Mabbott/ Governors

18. Development of the Policy

This policy will be reviewed after 1 year, or earlier in the light of any incidents or investigations, legislative changes or developments in best employment practice, to ensure its continuing relevance and effectiveness.

19. Appendices

1. Acceptable Use Policy (AUP) Staff and governors
2. Acceptable Use Policy (AUP) Students, Supply teachers, visitors, guests etc.
3. Acceptable Use Policy (AUP) Children
4. Parents letter
5. Image consent letter
6. Image consent form
7. Consent for images/ recordings at performances/ special events
8. Parental online safety awareness session letter
9. EYFS/ KS1 rules
10. KS2 rules
11. Incident log
12. Responding to an incident

APPENDIX 1

ICT Acceptable Use Policy (AUP) – Staff and Governors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs Mabbott.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in online safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of Mrs Mabbott.
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
13. I will report any known misuses of technology, including the unacceptable behaviours of others.
14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
19. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's online safety policy and help children to be safe and responsible in their use of ICT and related technologies.
20. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..

Date ……..

Full Name …….. (PRINT)

Position/Role ……..

APPENDIX 2

ICT Acceptable Use Policy (AUP) – Students, Supply Teachers, Visitors, Guests etc.

To be signed by any adult working in the school for a short period of time.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
3. I will not use any external device to access the school's network e.g. pen drive.
4. I will respect copyright and intellectual property rights.
5. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
6. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
7. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
8. I will not install any hardware or software onto any school system.
9. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..

Date ……
Full Name …… (PRINT)

Position/Role ……

Appendix 3

ICT Acceptable Use Policy (AUP) - Children

These rules reflect the content of our school's online safety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

- ✓ I will only use ICT in school for school purposes.
- ✓ I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
- ✓ I will only use the Internet and/or online tools when a trusted adult is present.
- ✓ I will only use my class e-mail address or my own school email address when emailing.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- ✓ I will not deliberately bring in inappropriate electronic materials from home.
- ✓ I will not deliberately look for, or access inappropriate websites.
- ✓ If I accidentally find anything inappropriate I will tell my teacher immediately.
- ✓ I will only communicate online with people a trusted adult has approved.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not give out my own, or others', details such as names, phone numbers or home addresses.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will not arrange to meet anyone that I have met online.
- ✓ I will only open/delete my own files.
- ✓ I will not attempt to download or install anything on to the school network without permission.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my online safety.
- ✓ I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

……**Parent/ Carer Signature**

We have discussed this Acceptable Use Policy and

…….. [Print child's name] agrees to follow the online safety rules and to support the safe use of ICT at St Michael and St John's School.

Parent /Carer Name (Print) ……

Parent /Carer (Signature) …… ……

Class …… Date……

This AUP must be signed and returned before any access to school systems is allowed.

St Michael & St John's RC Primary School
Lowergate, Clitheroe, Lancashire BB7 1AG
Headteacher: Mrs Zoe Mabbott BEd (Hons) NPQH

Telephone: 01200 422560
E-mail: bursar@ssmj.lancs.sch.uk

Appendix 4 ICT Acceptable Use Policy (AUP) Parent's letter <Date>

Dear Parent/Carer,

The use of ICT including the Internet, e-mail, learning platforms and mobile technologies are integral elements of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate. This is particularly relevant when using Social Network Sites that incorporate age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of the site's privacy policy and / or terms and conditions and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School online safety Policy and alongside the school's Behaviour and Safeguarding Policies outlines those principles we expect our children to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible. Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school.

Along with addressing online safety as part of your child's learning, we will also be holding Parental online safety Awareness Sessions during the school year and I would take this opportunity to strongly encourage your attendance wherever possible. Further information on these sessions will be communicated as soon as dates are confirmed. In the meantime, if you would like to find out more about online safety for parents and carers, please visit the Lancsngfl online safety website http://www.lancsngfl.ac.uk/online safety

If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact Mr Duckworth

Yours sincerely,

Mrs Z. Mabbott Headteacher

St Michael & St John's RC Primary School
Lowergate, Clitheroe, Lancashire BB7 1AG
Headteacher: Mrs Zoe Mabbott BEd (Hons) NPQH

Telephone: 01200 422560
E-mail: bursar@ssmj.lancs.sch.uk

Appendix 5- Parents letter for taking photographs

Date

Dear Parent / Carer

We regularly take photographs/videos of children at our school and believe that these can provide a valuable record of children's learning. These may be used in children's learning journeys and profiles, our school prospectus, in other printed publications, on our school website, or in school displays.

We also actively encourage children to use school cameras to take photographs / videos as part of their learning activity.

Occasionally, our school may be visited by the media or third party who will take photographs/videos of an event or to celebrate a particular achievement. These may then appear in local or national newspapers, websites or on televised news programmes.

We recognise that increased use of technology and opportunities for online publishing mean that there is greater potential for accidental or deliberate misuse. We endeavour to minimise risks by putting safeguards in place that will protect your child's interests, and enable us to comply with the Data Protection Act (1998).

Please read and complete the attached consent form (for each child) and return to school as soon as possible. We appreciate that some families may have additional concerns and anxieties regarding protection of a child's identity and therefore request that you inform us, in writing, of any special circumstances either now or at any time in the future that may affect your position regarding consent. Yours sincerely

Z. Mabbott

Mrs Z. Mabbott Headteacher

APPENDIX 6

Image Consent Form

Name of child's parent/ carer: _____

Name of child: _____

Year group: _____

Please read the Conditions of Use on the back of this form then answer questions 1-4 below. The completed form (<u>one for each child</u>) should be returned to school as soon as possible. (Please Circle your response)

1. Do you agree to photographs / videos of your child being taken by authorised staff within the school?
   Yes / No
2. Do you agree to photographs / videos of your child being taken in group situations by 3rd parties at special events e.g. School productions or extra- curricular events or in the EYFS setting?
   Yes / No
3. May we use your child's image in printed school publications and for digital display purposes within school?
   Yes / No
4. May we use your child's image on our school's online publications e.g. website/ Twitter/ Facebook?
   Yes / No
5. May we record your child on video? Yes / No
6. May we allow your child to appear in the media as part of school's involvement in an event? Yes / No

In signing this form you are also agreeing not to place images/ videos of children (other than your own) on social media sites such as Facebook and Twitter without specific permission from the parents of all the included children?

I have read and understand the conditions of use attached to this form

Parent/Carer's signature: ……

Name (PRINT): ……

Date: ……..

Conditions of use:

1. This form is valid for this academic year 2025 26
2. The school will not re-use any photographs or videos after your child leaves this school without further consent being sought.
3. The school will not use the personal contact details or full names (which means first name **and** surname) of any pupil or adult in a photographic image, or video, on our website or in any of our printed publications.
4. If we use photographs of individual children, we will not use the full name of that pupil in any accompanying text or caption.
5. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.
6. We will only use images of children who are suitably dressed and in a context that is not open to misinterpretation.
7. 3rd Parties may include other children's parents or relatives e.g. attending a school production.
8. Images / videos will be stored according to Data Protection legislation and only used by authorised personnel.
9. Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.

Notes on Use of Images by the Media

If you give permission for your child's image to be used by the media then you should be aware that:

1. The media will want to use any images/video that they take alongside the relevant story.
2. It is likely that they will wish to publish the child's full name, age and the school's name in the caption for the picture (possible exceptions to this are large group or team photographs).

It is possible that the newspaper will re-publish the story on their website or distribute it more widely to other newspapers or media organisations.

St Michael & St John's RC Primary School
Lowergate, Clitheroe, Lancashire BB7 1AG
Headteacher: Mrs Zoe Mabbott BEd (Hons) NPQH

Telephone: 01200 422560
E-mail: bursar@ssmj.lancs.sch.uk

Appendix 7 - Consent Form for Images to be Taken e.g. at a School Production or Special Event

Dear parent/ Carer

Your child will be appearing in annual school productions such as Christmas and Easter concerts. We are aware that these events are special for children and their relatives / friends and form treasured memories of their time at school.

We have a rigorous policy in place with regard to taking, using and publishing images of children and you have already signed a consent form stating whether you agree to your child's images / video being used in general circumstances.

Many parents / carers like to take photographs / videos of their children appearing in school productions, but there is a strong possibility that other children may be included in the pictures. In these circumstances, we request specific consent for images / videos to be taken by a third party (i.e. other parents). We need to have permission from all parents / carers of children involved in the production to ensure that they are happy for group images / videos to be taken and I would be grateful if you could complete the slip at the bottom of this letter and return to school as soon as possible.

We would also request that images / videos including other children or adults are not posted online, especially on Social Media sites e.g. Facebook without the specific permission of the individuals included in the footage.

Should any parents / carers not consent, we will consider other options, e.g. arranging specific photo opportunities after the production.

These decisions are not taken lightly, but we have to consider the safeguarding of all our children and respect parents' rights to privacy.

Yours sincerely,

Mrs Mabbott

(Headteacher)

_____

Child's name: _____ Date: _____

I agree/ do not agree to photographs/ videos being taken by third parties at the annual productions.

Signed: _____ (parent/ carer) Print name: _____

St Michael & St John's RC Primary School
Lowergate, Clitheroe, Lancashire BB7 1AG
Headteacher: Mrs Zoe Mabbott BEd (Hons) NPQH

Telephone: 01200 422560
E-mail: bursar@ssmj.lancs.sch.uk

Appendix 8 – Letter to parents regarding Parental online safety Awareness Session

<date>

Dear Parent/Carer,

Having access to online information and the opportunities that the digital world can offer has many benefits and for some it plays an important part of our everyday lives. However, as technology moves on at such a pace, it is sometimes difficult to keep up with new trends and developments, particularly with regard to mobile/games technologies and secure and safe accessibility to online material.

Our school has policies in place to ensure our children are learning in a safe and secure environment which includes being safe online. This session has been organised to help you to contribute to the process of helping your child to be aware of the potential risks associated with using the Internet and modern technologies.

Ofsted increasingly view Parental online safety Awareness sessions as essential components of effective safeguarding provision and I would therefore appreciate your support in attending this event.

We will be hosting the above session on the Date/Time below and I would strongly encourage your attendance

Date: …….. Time:……

The session will include reference to the following areas with time for you to ask questions:

- ✓ What are our children doing online and are they safe?
- ✓ Do they know what to do if they come across something suspicious?
- ✓ Are they accessing age-appropriate content?
- ✓ How can I help my child stay safe online? Yours sincerely,

Z. Mabbott

Mrs Z. Mabbott

Headteacher

I / we will be attending the above Parental online safety Awareness Session Name(s):……

Name and class of child: ……

Appendix 9

Classroom online safety Rules (EYFS/ KS1)

Our Golden Rules for Staying Safe with ICT

We only use the Internet when a trusted adult is with us.

We are always polite and friendly when using online tools.

We always make careful choices when we use the Internet.

We always ask a trusted adult if we need help using the Internet.

We always tell a trusted adult if we find something that upsets us.

Appendix 10

Classroom online safety Rules (KS2)

Our Golden Rules for Staying Safe with ICT

We always ask permission before using the Internet.

We only use the Internet when a trusted adult is around.

We immediately close/ minimise any page we are uncomfortable with (or if possible switch off the monitor).

We always tell an adult if we see anything we are uncomfortable with.

We only communicate online with people a trusted adult has approved.

All our online communications are polite and friendly.

We never give out our own, or other's personal information or passwords and are very careful with the information that we share online.

We only use programmes and content which have been installed by the school.

Appendix 11

Online safety Incident Log

All online safety incidents must be recorded by the designated person (Headteacher/ Deputy DSL/Online Safety Lead). This incident log will be monitored and reviewed regularly by the Headteacher and Chair of Governors.

Date / time of incident	Type of Incident	Name of pupils/ and staff involved	System details	Incident details	Resulting actions taken and by whom and signed
Jan 2010 9.50 am	Accessing Inappropriate Website	A N Other (Pupil) A N Staff (Class Teacher)	Class 1 Compute r 1.5	Pupil observed by Class Teacher deliberately attempting to access adult websites.	Pupil referred to Headteacher and given warning in line with sanctions policy for 1st time infringement of AUP. Site reported to LGFL as inappropriate.

Appendix 12

Responding to online safety Incident / Escalation Procedures