St. Michael's Catholic Primary & Nursery School

E Safety and ICT Policy

E Safety, ICT and Internet Policy

ICT equipment and the internet offer incredible opportunities for promoting and extending learning. In this school we will make best use of these tools to promote excellence and enjoyment. With the use of ICT and the Internet comes risk. We will do all we can to ensure that the internet and ICT is used safely and acceptably by all in school for the purposes that we intend. We understand the responsibility we have to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills needed to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The school's e-safety policy will operate in conjunction with other policies ie Behaviour Policy, Anti Bullying, GDPR and Safeguarding and Child Protection Policy.

Roles and Responsibilities

The Head teacher is the school's e Safety coordinator and also the Designated Safeguarding Person as the roles overlap.

All members of our school community will be involved in developing an understanding of the benefits of e-safety, its potential risks and its acceptable use.

E-Safety is recognised as an essential aspect with key staff involved having received **CEOP (Child Exploitation and Online Protection**) training and **all staff** having received **Prevent Duty Training.**

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.

All staff should be familiar with the school's policy including:

- Safe use of e-mail. It is imperative that only official school email addresses are used.
- Safe use of the Internet
- Safe use of the school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of pupil information/photographs on the school website and Instagram account

- Procedures in the event of misuse of technology by any member of the school community (see appendices)

- Their role in providing e-safety education for pupils.

Staff are reminded/updated about e-safety regularly and new staff receive information on the school's acceptable use policy as part of their induction. Supply Teachers must sign an acceptable use of ICT agreement before using technology equipment in school (see appendix 3 for staff acceptable use code of conduct).

Managing the school e-safety messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be shared with new staff, including the acceptable use policy as part of their induction.
- E-safety posters will be prominently displayed all over school.
- Parents and carers attention will be drawn to the School e-safety policy in newsletters, the school prospectus and on the school's Learning Platform.
- The school will make parents aware of e-safety issues through the School's Website, Instagram, newsletter and school events.
- The school will publish their Acceptable Use policy which outlines rules and sanctions for the use of the Internet and emerging technologies.
- The Governing Body understand the risks related to the Internet and associated technologies and are kept informed through discussions with the Headteacher.
- The Governors will monitor and review the implementation of the e-safety policy and procedures.

Curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new ways to promote e-safety. We provide opportunities within a range of curriculum areas to teach about e-safety.

- Educating pupils on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise and as part of the curriculum.

- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling, and activities as part of the ICT curriculum.

- Pupils are aware of the impact of online bullying through PSHE and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

- Professional Theatre companies in school to perform to promote internet /social media safety

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly through our technical support agreement with Halton Borough Council and 247 Technology Ltd.
- Virus protection will be purchased for each PC/Laptop and updated regularly.

- Web filtering will be provided through the 247 Technology Ltd. Any inappropriate sites accessed will be reported immediately to the Headteacher and the ICT Coordinator and the LA via the school's helpdesk.

- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.

- It is the responsibility our designated 247 colleague, to ensure that anti-virus protection is installed and kept up to date on all school machines.

- Any changes to filtering must be authorised by a member of the senior leadership team.

- Students will have supervised access to Internet resources through the school's fixed and mobile internet technology.

- Staff will preview any recommended sites before use.

- Raw image searches are discouraged when working with pupils.

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise any further research.

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

- Staff or pupil personal contact information will not be published. The contact details given online will be the school office e-mail.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that images cannot be misused. The majority of our photographs will be of groups of children unless the context relates to an individual.
- Pupils'' full names will not be used anywhere on the school's Learning Platform or other on-line space, particularly in association with photographs.

- Parental consent will be obtained before photographs/videos of pupils are published on the school's website or used in newsletters,

Social Networking and personal publishing

- Pupils will be educated in their use of social networking sites both in school and outside school so they can make informed decisions and understand the risks involved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

- Parents will be reminded annually that the minimum age for the use of social network is 13 and to be aware of any sites their children are accessing from home and the dangers attached.

- For further information regarding social media at St Michael's please see Social Media Policy.

Managing emerging technologies

- Pupils will be taught to be sensible, informed users of the internet
- The senior leadership team note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Staff must be aware that games machines such as the Sony Playstation, Nintendo DS and Microsoft Xbox have Internet access which may not include filtering, care will be required if pupils are permitted to bring them into school.

- All staff and learners understand that the school's ICT equipment must only be used for its intended purpose and not for personal use.
- School equipment must not be used for accessing personal and social networking sites.
- Personal, portable storage devices must not be attached to school equipment.
- Staff and pupils are aware they must act promptly if a discovery of inappropriate use found or if a disclosure is made.
- Parents and any appropriate authorities are informed where there is evidence of unacceptable use of ICT.
- Any cyber bullying of staff or pupils, in or out of school, must be reported and then investigated rigorously, in conjunction with any relevant authority including the police if appropriate.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to GDPR Act 2018.

Authorising Internet access

- All staff must read and sign the Acceptable Use Policy Statement before using the school's ICT resources.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Parents will be asked to discuss the Acceptable Use Policy Statement (rules and sanctions) with their child and sign to give their consent.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Halton LA can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the Headteacher who is also the eSafety coordinator and Designated Safeguarding Officer.
- Any complaint about staff misuse must be referred to the Headteacher and Chair of the School Governors.
- Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures. Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Incidents should be tracked (appendix 4)

The ICT Policy including E Safety will be reviewed every 2 years by The Governing body and signed by Chair of Governors, Mike Volynchook, on behalf of the Governing body.

Signed Copy available from school office.

Signed June 2026

Appendix 1

St Michael's Catholic Primary School

Staff Governor and Visitor Acceptable Use Policy

Introduction

ICT in its many forms-Internet, email, mobile devices etc – are now part of our daily lives. It is our duty to ensure that they are used safely and responsibly. All staff at St Michael's C.P. School are aware of the following responsibilities:

- All staff, Governors and visitors understand that it is a disciplinary offence to use the school ICT equipment for any purpose not permitted by the school.
- All staff, Governors and visitors understand that ICT includes a wide range of systems, including mobile phones, digital cameras, laptops and tablets.
- No staff, Governors or visitors will disclose any passwords provided to them by the school.
- Staff, Governors and visitors will not install any hardware or software on school owned device without the head's permission.
- All staff, Governors and visitors understand that they are responsible for all activity carried out under their username.
- All staff, Governors and visitors understand that their use of the internet may be monitored and if anything untoward is uncovered, could be logged and used in line with any disciplinary procedures. This includes all school owned devices. If an E-Safety incident should occur, staff will report it to the senior or Deputy Designated Professional for Child Protection as soon as possible.
- All staff, Governors and visitors will only use the school's email / internet / intranet etc and any related technologies for uses permitted by the Head or Governing Body. If anyone is unsure about an intended use, they should speak to the Head beforehand. If staff are using a personal email address for school business, this will have been on approval from the Headteacher.
- All staff, Governors and visitors will ensure that data is kept secure and is used appropriately as authorised by the Head or Governing Body. No passwords should be divulged and memory sticks should also be encrypted.
- Personal devices must only be used in the context of school business with the explicit permission of the head. Personal mobile phones or digital cameras must not be used for taking any photographs related to school business. Each class has a phone specifically for this purpose. The school phone is also to be used for any off-site visits.

- All staff, Governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- All staff, Governors and visitors using AI searches will not enter any confidential student information or other personal school information in any searches.
- All staff, Governors and visitors using school equipment will only use the approved email system for school business as agreed with the Head teacher and Governors.
- Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use. At the start of each year, our parents are asked to sign if they agree to their children's images being used in our brochure or in the local press. If a parent does not agree to this, we ensure that their child's photograph is not used. Filming and photography by parents and the wider community at school events such as sports days and school procedures must be in agreement with School procedures.
- All staff, Governors and visitors will make every effort to comply with comply and intellectual property rights.
- All Staff, Governors when using social media will not negatively refer to the school, the staff or any school business, maintaining their professional role at all times.
- All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Head or the Deputy Designated Professional in line with our school's Safeguarding Policy.

I acknowledge that I have received a copy of the Acceptable Use Code of Conduct.

Full Name……
Signature……..**Date**…….

Appendix 2

St Michael's E-Safety

Incident Log

Details of ALL e-safety incidents to be recorded in the Incident Log by the e-safety co-ordinator. This incident log will be monitored termly by the e-safety co-ordinator and Head teacher.

Date & time	Name of pupil or staff member	Room and computer/device	Details of incident (including evidence) number	Actions and reasons

Appendix 3

St Michael's Catholic Primary School's School E-Safety Code Think then click……	
	We ask permission before using the internet
	We only use websites our teacher has chosen
	We tell an adult if we see anything we are uncomfortable with
	We immediately close any webpage we are uncomfortable with
	We only email people an adult has approved
	We send emails that are polite and friendly
	We never give out personal information or passwords
	We never arrange to meet anyone we don't know
	We do not open emails sent by anyone we don't know