ST MARY MAGDALENE CATHOLIC PRIMARY SCHOOL

COMPUTING POLICY
Including E-Safety, Acceptable Use & Curriculum Policies

'Growing Together in Faith & Love'

March 2025

Contents

Mission Statement and School Aims

"Growing Together in Faith and Love"

As a Christian community, school life is based on the Gospel and the teachings of the Catholic Church. Every child is encouraged towards high ideals and equal opportunity is given to all pupils to develop their talents to the full.

At the heart of our community is Jesus Christ, everything we do is underpinned by or school mission statement "Growing Together in Faith and Love". Everyone in our community is valued and respected.

School Aims

- To ensure that all children appreciate that they are unique – ***a gift from God.***
- To foster development of the whole child as a person, including economic awareness, to enable them to become responsible citizens of the future.
- To provide a caring and compassionate community where each individual feels valued and safe.
- To provide a learning environment that is attractive, welcoming, stimulating and enables all to enjoy and achieve.
- To foster a commitment to excellence in all things, so that each child fulfils their potential.
- To ensure that the special educational needs of the individual pupils are an integral part of all aspects of school life.
- To support parents to keep their children safe online, by raising awareness of internet safety.
- To provide a variety of teaching and learning approaches to cater for the needs and abilities of all our pupils.
- To minimise incidents involving cybersecurity.
- To endeavour to do our best for our pupils in partnership with parishes and parents.
- To seek to serve the welfare of families who make up the school community.
- To promote healthy eating, good physical and mental health and promote healthy life styles.
- To work in partnership with the Diocese of Northampton and Milton Keynes Council.
- To provide an efficient and cost-effective school, thus providing value for money.
- To eliminate unlawful racial discrimination and promote equal opportunities, and good race relations in all areas of school life.

Introduction

St. Mary Magdalene Catholic Primary School recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play, but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

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

Responsibilities

The Headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. This includes having adequate filtering and monitoring arrangements in place, which is regularly reviewed and to appoint an individual to lead on day to day use in school. The named eSafety lead and computing coordinator in this school is Gabrio Thonet.

All breaches of this policy must be reported to the eSafety lead and computing coordinator, Gabrio Thonet. All breaches of this policy that may have put a child at risk must also be reported to a designated safeguarding lead (please see appendices H-K).

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

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

Scope of policy

The policy applies to:

- Pupils
- Parents/carers
- Teaching and support staff
- School governors
- Peripatetic teachers/coaches, supply teachers, student teachers
- Visitors
- Volunteers
- Voluntary statutory or community organisations using the school's facilities

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

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

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: Safeguarding, Keeping Children Safe in Education, GDPR, health and safety, home–school agreement, home learning, behaviour, anti-bullying and PSHCE/RSE policies.

Policy and procedure

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

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

The filtering and monitoring system is designed to pick up on any access to inappropriate websites or content on any device used with the school system including emails. Staff are made aware of this at induction and reminded on a regular basis.

Use of email

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

Staff, governors and pupils should only open emails or attachments from trusted sources, not open emails or attachments from suspect sources and should report their receipt to the eSafety lead and computing coordinator, Gabrio Thonet. If there is any doubts then Gabrio Thonet must be contacted.

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

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.
- Staff must only use pre-approved systems if creating blogs, wikis or other online content.
- When working with pupils, searching for images should not be done ‘live’, the screen should be off or frozen, to add another layer of protection. Only use the school system to access the internet or send emails.

Users must not:

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

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any website promoting misogyny, hatred towards different groups.
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect
- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school
- Share their password with anyone else or allow others to use a device they are logged into.

Only a school device may be used to conduct school business outside of school. The only exception would be where permission has been granted by the Headteacher, Rosemarie Jones.

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

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the eSafety Lead and computing coordinator, Gabrio Thonet.

Storage of Images

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

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by the school eSafety Lead and computing coordinator, Gabrio Thonet. Staff and pupils may have temporary access to photographs taken during a class/trip session, but these will be transferred/deleted promptly.

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

Staff and other professionals working with pupils, can only record images of pupils (whether on or off site) where permission has been granted, and on equipment approved, by the Headteacher, Rosemarie Jones, and/or the school eSafety Lead and computing coordinator, Gabrio Thonet. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

Use of personal mobile devices (including phones)
The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas, times and circumstances (these are detailed in the school mobile phone policy). Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers may use personal mobile phones and devices whilst on the school site, provided this is courteous and appropriate to the school environment. We allow parents to photograph or video school events such as shows or sports day, using personal mobile phones/devices- but parents may not publish images/videos (e.g. on social media sites) that include any children other than their own. The acceptable use of ICT policy is given to all new parents to sign and agree to. Staff will challenge other members of staff/governors/volunteers/visitors/parents/contractors who use their mobile phone whilst children are present. This will then be reported to senior staff.

Pupils are allowed to bring personal mobile devices/phones to school upon parental request, but must turn these off and hand them into the office on arrival. These will be stored in a safe place and collected by the child upon leaving the school. Pupils are not permitted mobile phones on school day/residential trips.

Under no circumstance should pupils use their personal mobile devices/phones to take images of:

- Any other pupil, unless they and their parents have given agreement in advance
- Any member of staff

The school is not responsible for the loss, damage or theft on school premises of any personal mobile device. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device. Personal mobiles must never be used to access school emails and data. The only exception would be where permission has been granted by the Headteacher, Rosemarie Jones.

New technological devices

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

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to a designated safeguarding lead (DSL), and eSafety lead and computing coordinator, Gabrio Thonet (please see appendices H-K). Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

The opening of an email or alert which can be seen by parents, staff or children is prohibited. Staff must only open confidential emails and safeguarding alerts when it cannot be overseen.

Filtering and monitoring

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure risks from the school's or college's IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

Our school uses 'Protex Web filtering'. According to the UK Safer Internet Centre's Filtering Provider Checklist Responses, Protex fully meets all of the criteria for the nationally defined 'appropriate filtering standards'. Pupil filtering is set to the strictest level (primary). If a user attempts to search for, or access a site blocked by Protex, this generates a near real-time alert that is sent to all teaching staff in the school. Staff will then identify the pupil (through access of the search history) and respond according to the school safeguarding policy (please also see appendices H-K). In addition, the school's eSafety Lead and computing coordinator, Gabrio Thonet receives a once a day summary/digest report of any blocked activity.

The Protex system is tested by the school's eSafety Lead and computing coordinator, Gabrio Thonet on a regular (at a minimum weekly) basis. This involves 3 tests recommended by Protex to ensure that: 1. unfiltered internet is blocked by Protex, 2. age appropriate Protex filtering profiles are applied across the school, 3. Protex filtering content check is active.

Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive, age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE, and Relationships and Health Curriculum are central in supporting the delivery of online safety education.

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

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

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity

- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment

- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)

- Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others

- Understanding the permanency of all online postings and conversations

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

- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help

- How the law can help protect against online risks and abuse

Computing Timetabling

Currently, the computing curriculum is taught as an explicit subject, although teaching of computing objectives may frequently be embedded throughout the curriculum so that computing activities are undertaken in meaningful, challenging contexts.

Computing in the school can either be taught in the form of 1 hour (or longer) sessions each week or as a topic during a computing week each term. This can take the form of computing used as a tool for learning or as an identified computing lesson. We aim to teach children to type; it is not acceptable to teach children only handwriting skills in an age where typing is the dominant method of recording. Typing activities using online games and teaching should be undertaken as part of the computing curriculum. It is our belief that all children's needs should be met in line with our Equal Opportunities policy. Children of all abilities must be challenged and supported.

Staff may use other opportunities, discussions or incidents to raise awareness on internet safety and appropriate behaviour.

Scheme of Work

The curriculum is delivered via the Purple Mash Computing Scheme of Work, although other resources and scheme materials can be used to augment and extend the curriculum (e.g. BBC Microbit Coding). Teachers should ensure that computing is planned into the curriculum in advance, offering high-quality learning experiences within the computing programme of study.

Predominant Computing strand (most units will include aspects of all strands):

	Computer Science
	Information Technology
	Digital Literacy

Rather than a scheme with set lessons, the early years resources are designed to integrate into the day-to-day routine and set-up of an early years setting with opportunities for using Mini Mash or Purple Mash as part of the Early Years curriculum to support children in working towards early learning goals. In addition, there are units of suggested ideas that focus on computing skills specifically, that can also be provided as opportunities for learning as part of the topics in other areas to give children a sound basis to explore topics using technology and to be ready for progressing through the Computing curriculum. These are as follows and are designed to be integrated and linked to wider early years curriculum areas. These have been loosely classified into three streams but there is overlap between all three streams.

Mouse and Trackpad Skills	Keyboard Skills	Drawing skills	Robots	Sounds	Photography
Technology Around Us	Hardware	Safety and Privacy	Quizzes	Using Purple Mash with an Individual Login	

Year 1

	Unit 1.1	Unit 1.2	Unit 1.3	Unit 1.4	Unit 1.5	Unit 1.6	Unit 1.7	Unit 1.9
	Online Safety & Exploring Purple Mash	Grouping & Sorting	Pictograms	Lego Builders	Maze Explorers	Animated Story Books	Coding	Technology outside school
Number of lessons	4	2	3	3	3	5	6	2
Main tool			2Count		2Go	2Create A Story	2Code	

Year 2

	Unit 2.1	Unit 2.2	Unit 2.3	Unit 2.4	Unit 2.5	Unit 2.6	Unit 2.7	Unit 2.8
	Coding	Online Safety	Spreadsheets	Questioning	Effective Searching	Creating Pictures	Making Music	Presenting Ideas
Number of lessons	6	3	6	5	3	5	3	4
Main tool	2Code		2Calculate	2Question 2Investigate		2Paint A Picture	2Sequence	

Year 3

	Unit 3.1	Unit 3.2	Unit 3.3	Unit 3.4	Unit 3.5	Unit 3.6	Unit 3.7	Unit 3.8	Unit 3.9	Unit 3.10
	Coding	Online safety	Spreadsheets	Touch Typing	Email (inc. email safety)	Branching Databases	Simulations	Graphing	Presenting	micro: bit
# lessons	6	3	6	4	6	4	3	2	5\6*	4
Main tool	2Code		2Calculate	2Type	2Email	2Question	2Simulate	2Graph	Power Point or Google Slides	Free code micro: bit

*Platform dependent

Year 4

	Unit 4.1	Unit 4.2	Unit 4.4	Unit 4.5	Unit 4.6	Unit 4.7	Unit 4.8	Unit 4.9	Unit 4.10	Unit 4.11
	Coding	Online Safety	Writing for Different Audiences	Logo	Animation	Effective Searching	Hardware	Making Music	Intro to AI	micro:bit
# lessons	6	4	5	4	3	3	2	4	4	4
Main tool	2Code			2Logo	2Animate			Busy Beats		Free code micro: bit

Year 5

	Unit 5.1	Unit 5.2	Unit 5.3	Unit 5.4	Unit 5.5	Unit 5.6	Unit 5.7	Unit 5.8	Unit 5.9	Unit 5.10
	Coding	Online Safety	Spreadsheets	Databases	Game Creator	3D Modelling	Concept Maps	Word Processing	External Devices	micro:bit
# lessons	6	3	6	4	5	4	4	7/8*	6	4
Main tool	2Code		2Calculate	2Investigate	2DIY 3D	2Design & Make	2Connect	MS Word or Google Docs	2Code Purple Chip	Free code micro:bit

*Platform dependent

Year 6

	Unit 6.1	Unit 6.2	Unit 6.4	Unit 6.5	Unit 6.6	Unit 6.7	Unit 6.8	6.9
	Coding	Online Safety	Blogging	Text Adventures	Networks	Quizzing	Understanding Binary	Spreadsheets
# lessons	6	2	4	5	3	6	4	8
Main tool	2Code		2Blog			2Quiz		Excel or Google Sheets

Resources

All classrooms have a master laptop which controls an Interactive Whiteboard. All classrooms have integrated stereo sound.

In school we have five trolleys of 30 Chromebook laptops for class-based computing and curriculum study. These are shared on a rota. We have two trolleys of 30 Apple iPads which are populated with learning apps suitable for all age-ranges. These are also rota-shared.

Staff have access to recording equipment and memory sticks. The memory sticks are encrypted and provided to assist them in planning, preparation and record-keeping. Other appropriate resources may also be used with the pupils, provided permission has been granted by the eSafety Lead and computing coordinator, Gabrio Thonet.

Staff have access to the school network. They are given password access while working in school and a space to store work-related files.

If any resources required to teach the curriculum expire or need to be purchased, staff must make the eSafety Lead and computing coordinator, Gabrio Thonet aware of this.

Assessment

Pupil attainment is assessed by staff, according for each of the 3 strands: Computer Science, Information Technology and Digital Literacy. Staff are assisted in this through use of the 2Simple Computing Assessment Tool for Years 1 to 6, which shows the Purple Mash units that correspond to each strand. Overall results are presented in end of year reports for each pupil and within the year group computing file. Teachers can access and assess any work that is submitted online by pupils, and attainment tracking informs their future planning.

Assessment is undertaken each session. Through use of lesson success criteria and/or progression of skills documents, both teachers and pupils can evaluate progress through self, peer and group assessment.

Work from a range of classes and abilities is shared using the Purple Mash Noticeboard. Pupils can also log onto accounts from home to see these or to add to or complete existing/extra activities, so can share and celebrate these with parents.

Teachers submit examples of computing work from their class. This is then stored in the year group computing file and handed in to the eSafety Lead and computing coordinator, Gabrio Thonet

Staff and Governor Training

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

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

Any organisation working with children based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix B).

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B).

Guidance is provided for occasional visitors, volunteers and parent/carer helpers (Appendices C and E).

Working in Partnership with Parents/Carers

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

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

Parents/carers are asked to read, discuss and co-sign with each child the Acceptable Use Agreement. Reminders of the agreement are sent to parents, for them to go through with their children, on an annual basis. A summary of key parent/carer responsibilities will also be provided and is available in Appendices C and E. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities.

Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. Online safety incident recording sheets can be found in appendices H, I and J.

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

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

Appendix A – Online Safety Acceptable Use Agreement – Staff, Governors and student teachers (on placement or on staff)

School name: St. Mary Magdalene Catholic Primary School
eSafety lead: Gabrio Thonet
Designated Safeguarding Leads (DSLs): Mrs Jones, Mrs Williams, Mr Jones, Mrs Messina, Mrs Ledger, Mrs Lighthill, Mrs Swaby

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

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

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the eSafety lead and computing coordinator Gabrio Thonet, a designated safeguarding lead and an incident report completed (please see appendices H-K).

Online conduct

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

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

I will report any accidental access to or receipt of inappropriate materials, or filtering breach to the eSafety lead and computing coordinator, Gabrio Thonet

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

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

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity, I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

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

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

Passwords

I understand that there is no occasion when a password should be shared with a pupil, visitor or staff member. In the event of it being seen or identified by someone else, I will immediately report it, so it can be changed. I understand that a record will be kept of any breach.

Data protection

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

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

- I will mark any emails with personal information as confidential
- I will not open any confidential emails or alerts unless I am certain it cannot be seen by anyone else. This includes opening alerts when connected to the whiteboard system.

Images and videos
I will only record and upload images of staff, pupils or parents/carers (whether on or off site) where permission has been granted, and on equipment approved, by the Headteacher, Rosemarie Jones, and/or the school eSafety Lead and computing coordinator, Gabrio Thonet. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file. I am aware that parent/carer permission to use images/videos of their child/ren is sought when they join our school, but that they have the right to deny this request.

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by the school eSafety Lead and computing coordinator, Gabrio Thonet. Staff and pupils may have temporary access to photographs taken during a class/trip session, but these will be transferred/deleted promptly.

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

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

During school hours, I will only use approved personal devices in designated areas and never in front of pupils. I will not access secure school information from personal devices without permission of the Headteacher, Rosemarie Jones. With regards to mobile phones, I'll follow the rules in the school's mobile phone policy.

Additional hardware/software
I will not install any hardware or software on school equipment without permission of the eSafety Lead and computing coordinator, Gabrio Thonet.

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

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to a designated safeguarding lead, and eSafety Lead and computing coordinator, Gabrio Thonet (please see appendices H-K).

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

If I am using the internet to teach about controversial issues, I will secure, on every occasion, approval in advance for the material I plan to use with the eSafety Lead and computing coordinator, Gabrio Thonet.

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

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

Signature ……..…….…… Date ……

Full Name ……..... (printed)

Job title ……...…….....……

Appendix B - Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers

School name: St. Mary Magdalene Catholic Primary School
eSafety lead: Gabrio Thonet
Designated Safeguarding Leads (DSLs): Mrs Jones, Mrs Williams, Mr Jones, Mrs Messina, Mrs Ledger, Mrs Lighthill, Mrs Swaby

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the school eSafety Lead and computing coordinator, Gabrio Thonet. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety, GDPR and mobile phone policies provide further detailed information.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to: the eSafety lead and computing coordinator Gabrio Thonet, a DSL and an incident report completed.

Online conduct

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

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

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the eSafety lead and computing coordinator, Gabrio Thonet.

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

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

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the eSafety lead and computing coordinator, Gabrio Thonet.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

Information can be shared with parents/carers through an organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

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

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos
I will only record and upload images of staff, pupils or parents/carers (whether on or off site) where permission has been granted, and on equipment approved, by the Headteacher, Rosemarie Jones, and/or the school eSafety Lead and computing coordinator, Gabrio Thonet. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file. I am aware that parent/carer permission to use images/videos of their child/ren is sought when they join our school, but that they have the right to deny this request.

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by the school eSafety Lead and computing coordinator, Gabrio Thonet. Staff and pupils may have temporary access to photographs taken during a class/trip session, but these will be transferred/deleted promptly.

Use of Email
I will only use my professional or formal student email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

Use of personal devices
I understand that when working in the school, I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher, Rosemarie Jones.

During school hours, I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning. Pupils can also be encouraged, but not required, to access such apps on their own devices if allowed by the school and with parent/carer agreement. With regards to mobile phones, I will follow the rules set out in the school's mobile phone policy.

Additional hardware/software
I will not install any hardware or software on school equipment without permission of the school eSafety Lead and computing coordinator, Gabrio Thonet.

Promoting online safety
I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any online safety behaviour (of staff, governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to a DSL, and eSafety Lead and computing coordinator, Gabrio Thonet (please see appendices H-K).

Classroom management of internet access
I will pre-check for appropriateness all internet sites used in the classroom or during a tutoring session; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If using the internet to teach about controversial issues, I will secure, on every occasion, approval in advance for the material I plan to use with the eSafety Lead and computing coordinator, Gabrio Thonet

Video conferencing
I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO, DSL and eSafety Lead and computing coordinator, Gabrio Thonet. A school owned device should be used when running video conferences, where possible.

User Signature
I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature ……..…….…… Date ……

Full Name ……..... (printed)

Job title/Role ……..……...……...……

Appendix C - Requirements for visitors, volunteers and parent/carer helpers working in the school (working directly with children or otherwise)

School name: St. Mary Magdalene Catholic Primary School

eSafety lead: Gabrio Thonet

Designated Safeguarding Leads (DSLs): Mrs Jones, Mrs Williams, Mr Jones, Mrs Messina, Mrs Ledger, Mrs Lighthill, Mrs Swaby

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with a DSL, and eSafety Lead, Gabrio Thonet.

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas, times and circumstances. When not in these, phones must be switched off and out of sight. Any exception must be pre-arranged. With regards to mobile phones, I will follow the rules set out in the school's mobile phone policy.

- I will not take images, sound recordings or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.

- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils and parent/carers. Where appropriate I may share my professional contact details with parents/carers provided a DSL is informed before I leave the school.

- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared online, including on social media sites.

- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the Headteacher, Rosemarie Jones.

- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use, I will check with my contact in the school.

Signature ……..…….…… Date ……

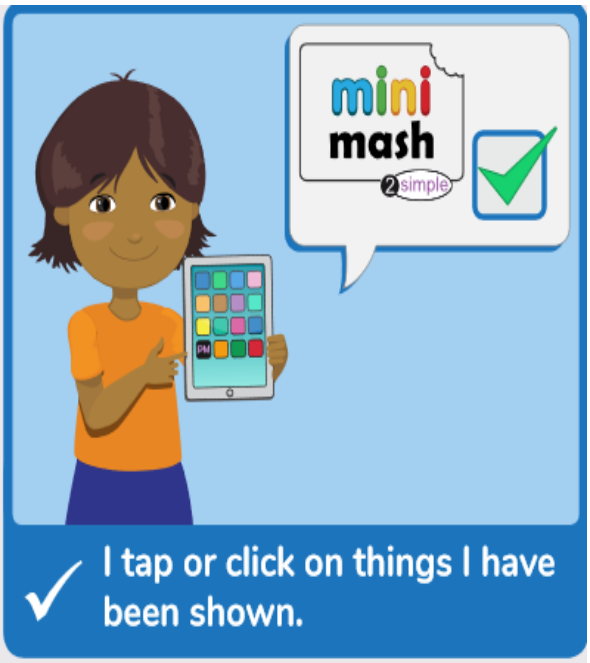
Full Name ……..... (printed)

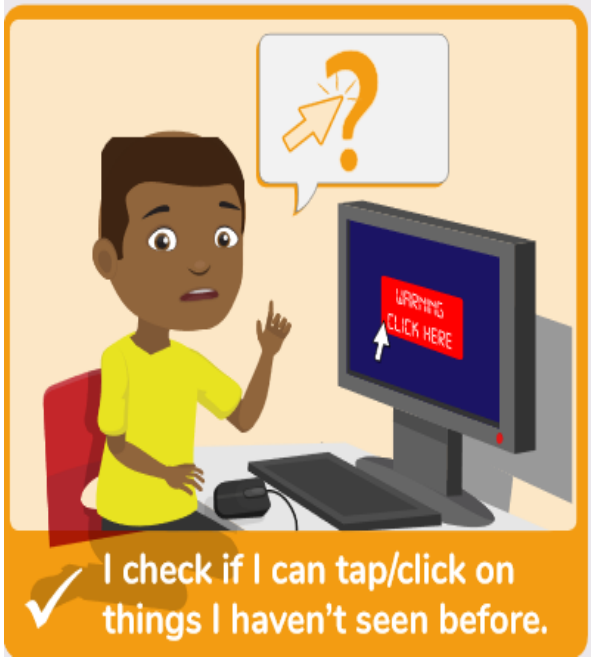
Job title/Role ……..……...……...……

Appendix D - Online Safety Acceptable Use Agreements - Primary Pupils

Online Safety Acceptable Use Agreement for EYFS Pupils

My online safety rules





Online Safety Acceptable Use Agreement for KS1 Pupils

My online safety rules

- ✓ I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.
- ✓ I only open activities that an adult has allowed me to use.
- ✓ I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- ✓ I keep my passwords safe and will never use someone else's.
- ✓ I know personal information such as my name, address and birthday should never be shared online.
- ✓ I know I must never talk with strangers online.
- ✓ I am always polite when I use the internet.
- ✓ I understand that these rules are to keep me safe. If I break the rules my teachers will look into it and may need to take action.

Online Safety Acceptable Use Agreement for KS2 Pupils

My online safety rules

- I will only use IT equipment in school for activities agreed by school staff and out of school for activities agreed by my parents/carers, and only with a trusted adult present.
- I will respect computing equipment and immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will not use a personal email address or other personal accounts in school.
- I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.
- In school I will only open or delete my files when told by a member of staff.
- I will not tell anyone other than my parents/carers my usernames and passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not comment/reply, but will tell my teacher or my parent/carer immediately.
- I will not give out my own or other people's personal information, including: name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- Even if I have permission, I will not look for, save, send or upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I will not assume that personal devices can be brought into school without getting permission. Any devices that can take pictures or make phone calls, such as mobile phones and smart watches, must be switched off and left at reception whilst I am on school premises. These devices are not permitted on school day/residential trips.
- I understand my behaviour in the virtual classroom should mirror that in the physical classroom.
- I will not lie about my age or access games, apps or social networks that are for older people, as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules, my teachers will look into it and may need to take action.

Dear Parent/Carer,
The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using IT. It is essential that children are aware of online risks, know how to stay safe and know where to go to report problems or to get help.

Please read through the relevant pupil online safety acceptable use agreement with your child/ren and ensure they understand their importance and what it means for them (and you). Then, parents/carers are to read though the parent/carer agreement. When you have done this, both pupils (year 1 and above) and parents/carers need to sign this agreement to say that you all agree to follow the rules. Any concerns or explanation can be discussed with the school eSafety Lead and computing coordinator, Mr Thonet, or Headteacher, Mrs Jones.

Please return the signed sections of this form which will be kept on record in school.

Pupil agreement

Pupil name …….…….…….

These rules are to keep me safe. I have talked about them with my parents/carers.
I know what the rules are and will follow them.

Pupil signature (for year 1 and above)
Pupils can just write their first name …..……..……..……..

Parent(s)/Carer(s) agreement
I/we have discussed this agreement, with my/our child/ren. I/we agree to support them in following the terms of this agreement.

I/we agree that should my/our child/ren need to access the Internet at home or anywhere else, that I/we will take all reasonable precautions to ensure they cannot access inappropriate materials and that they will use ICT and the Internet in an appropriate manner. I/we recognise that social networking sites such as Facebook, Twitter, Instagram, Snapchat, TikTok, Wink, Discord and Skype have a minimum age rating of 13. YouTube accounts require a person to be 13+ (though YouTube states that it can be used if children have parental/guardian permission), whilst WhatsApp has a minimum age rating of 16 (for the latest guidelines for the most popular sites, apps and games, please refer to https://www.commonsensemedia.org/app-reviews.)

I/we agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute. (Rather than posting negative material online, any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that the school can protect the reputation of staff, pupils and parents.

I/we agree that I/we do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.

I/we agree that any use that I/we make of mobile phones or devices whilst on the school site will be courteous and appropriate to the school environment and only at designated times and in designated areas.

I/we understand that whilst I/we may be given permission to take pictures/videos at school events such as shows or sports day, under no circumstance should any images/videos of any child other than my/our own be posted or published (e.g. on social media sites).

I/we agree that pupils may not use any devices that can take pictures or make phone calls, such as mobile phones and smart watches in school, or on school day/residential trips, and that these must be turned off and left at reception whilst on school premises. Furthermore, these are left at the owner's risk and the school is not responsible for any loss or damage.

I/we also agree that all cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school would then investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. I/we agree that no reply should ever be sent to the sender/poster of cyberbullying content. If applicable, I/we would block the sender and report abuse to the site. I/we would not forward the evidence, but would retain it and show it to the school and/or to the police.

Parent(s)/Carer(s) name(s)...…….……..……..

Parent/carer signature ……..……..…..……..……...

Date ……..……..…..……..……..

Appendix E - Online safety policy guide - Summary of key parent/carer responsibilities

The school provides eSafety information for parents/carers, through the website, newsletters and events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online. The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. Any concerns or explanation can be discussed with the school eSafety Lead and computing coordinator, Mr Thonet or Headteacher, Mrs Jones.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.
- Should their child need to access the Internet at home or anywhere else, parents/carers are required to take all reasonable precautions to ensure they cannot access inappropriate materials and that they will use ICT and the Internet in an appropriate manner. They should also recognise that social networking sites such as Facebook, Twitter, Instagram, Snapchat, TikTok, Wink, Discord and Skype have a minimum age rating of 13. YouTube accounts require a person to be 13+ (though YouTube states that it can be used if children have parental/guardian permission), whilst WhatsApp has a minimum age rating of 16 (for the latest guidelines for the most popular sites, apps and games, please refer to https://www.commonsensemedia.org/app-reviews.)
- Any parent/carer, concerned about an aspect of school should make immediate contact with a member of staff rather than posting concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.
- Parents/carers, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.
- Any use of mobile phones or devices, by parents/carers, whilst on the school site will be courteous and appropriate to the school environment and only at designated times and in designated areas.
- Whilst parents/carers may be given permission permission to take pictures/videos at school events such as shows or sports day, under no circumstance should any images/videos of any child other than their own be posted or published (e.g. on social media sites).
- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy. Any devices that can take pictures or make phone calls, such as mobile phones and smart watches, cannot be used by pupils in school or brought on school day/residential trips. These must be turned off and left at reception whilst on school premises. These are left at the owner's risk and the school is not responsible for any loss or damage.
- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.

Please see the full computing and eSafety policy in the policies section on the school website.

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

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

The following procedures are recommended:

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

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

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

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

If negative comments are posted:

- Collect the facts

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

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

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

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

- Addressing negative comments and complaints

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

The meeting must:

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

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

- Reporting the matter to the social network site if it breaches their rules or breaks the law;

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

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

Appendix H - Online safety incident reporting form

Any member of the school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to the eSafety Lead, Gabrio Thonet.

Name of person reporting incident:				
Signature:				
Date you are completing this form:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young people	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of acceptable use agreement, please specify			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, WhatsApp, Snapchat, Instagram etc.
Evidence of the incident	Specify any evidence available but do not attach.

Thank you for completing and submitting this form.

Appendix I - Online safety incident record

Name of person reporting incident:				
Date of report:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young person	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyberbullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of Acceptable Use Agreement			
Other, please specify			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, WhatsApp, Snapchat, Instagram etc.
Evidence of the incident	Specify any evidence provided but do not attach

Immediate action taken following the reported incident:	
Incident reported to eSafety Lead: Gabrio Thonet, and to a DSL	
Safeguarding advice sought, please specify	
Referral made to MK LADO	
Incident reported to police and/or CEOP	
Online safety policy to be reviewed/amended	
Parent(s)/carer(s) informed please specify	
Incident reported to social networking site	
Other actions e.g. warnings, sanctions, debrief and support	
Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery	

Brief summary of incident, investigation and outcome (for monitoring purposes)	

Appendix J - Online safety incident log

Summary details of ALL online safety incidents will be recorded on this form by the eSafety Lead, Gabrio Thonet or other designated member of staff. This incident log will be monitored at least termly and information reported to SLT and governors.

Date & time	Name of pupil or staff member Indicate target (T) or offender (O)	Nature of incident(s)	Details of incident (including evidence)	Outcome including action taken

Online Incident

Record actions at each stage of the process

Illegal Activity or Material found or suspected

Reported by broadband/filter provider

Reported to member of school staff who explains reporting process

If possible, turn off screen/ isolate device. Do not share material.

Inform Designated Safeguarding Lead → Headteacher Chair of Governors

Inform police (or CEOP www.ceop.police.uk/safety-centre if any difficulty making contact)

Content

Inform www.iwf.org.uk

Activity

Secure evidence and disable access

- School work with partners to understand incident
- Strategy agreed and implemented

Child(ren)

Instigator

Disciplinary sanctions according to school policy. Provide appropriate support

Victim

Provide appropriate support and legal advice for staff

Staff

Instigator

Contact LADO / HR Disciplinary sanctions according to school policy

Illegal means something against the UK Criminal Law such as:

Creating, downloading or distributing child sexual abuse images (Further advice on this from www.gov.uk)

Inciting race , homophobic, religious hatred or other hate crime

eLIM Support Services for Education — sse

Further support and training can be obtained by contacting:

mailto:elimadmin@somerset.gov.uk

Harmful/Inappropriate activity or material found or suspected

Incident could be:

- Upsetting or bullying through technology
- Accessing websites against school policy
- Using personal device in class without permission

Child(ren)

Victim

Cyberbullying

- Always listen, capture evidence, and report
- Record and take action according to anti-bullying/ peer-on-peer abuse policy

Inappropriate Content

- Turn off/minimise screen, isolate device
- Ask another adult to review with you
- Ensure site/images are added to school filtering system and report to reportharmfulcontent.com
- Review incident with child(ren) if appropriate
- Record and inform parents

Inappropriate Gaming

- Record impact on child
- Discuss with parents
- Provide appropriate support

Radicalisation and Extremism

- Assess nature and extent of risk
- Record and report https://www.milton-keynes.gov.uk/adult-social-care/safeguarding-adults-and-children/prevent
- Develop appropriate support for child(ren)

Instigator

Cyberbullying including unacceptable contribution to a webpage, blog, social network, app or text

- Capture screen shot as evidence including the name of the contributor
- Delete, or ask child(ren) to delete the contribution
- Discuss contribution with child(ren) involved as appropriate
- Take action according to school's anti-bullying/ peer-on-peer abuse policy including discussing contribution with child(ren) involved and informing parents as appropriate

Deliberate searching for and sharing of inappropriate content

- School device: Identify child(ren) involved, with support from technician
- Personal device: Confiscate and use right to search
- Record and take action according to school's behaviour policy
- Inform parents

Staff

Victim

Adult(s) as Instigator

- Contact the person involved and administrator where a closed group, invite into school to discuss
- Request the offending material be removed
- Inform governors and consider written communication
- Provide support
- Report to website/social network

If there is no resolution, or you need help, contact the **Professional Online Safety Helpline**

Child(ren) as Instigator

- Contact the child(ren) involved
- Request the offending material be removed
- Inform the parents
- Establish appropriate restorative action
- Provide support
- Report to website/social network

If there is no resolution, or you need help, contact the **Professional Online Safety Helpline**

Instigator

Child as Victim

If a member of staff has:

- *Behaved in a way that has, or may have harmed a child*
- *Possibly committed a criminal offence*
- *Behaved towards a child in a way which indicates s/he is unsuitable to work with children*

Review evidence and **Contact LADO within one working day**

- Follow school disciplinary procedures and contact HR officer
- Where Head teacher is involved immediately contact Chair of Governors

Staff as Victim

- Refer to the signed, Acceptable Use Agreement/Professional Code of conduct
- Follow school disciplinary procedures and contact HR officer
- Contact Chair of Governors

Local Contact Details:

School Designated Safeguarding Leads: 1: Mrs. Jones. 2: Mrs. Williams.
3: Mr. Jones. 4: Mrs Messina 5: Mrs. Ledger. 6: Mrs. Lighthill.
School eSafety Lead: Gabrio Thonet
Safeguarding Governor: Mrs. Jones

NSPCC / O2 Online Safety help for families

0808 8005002

Professional Online Safety Helpdesk

0344 381 4772

helpline@saferinternet.org.uk

Record as a **child protection concern** and/or separate online safety incident according to school policy Provide appropriate support for those involved in incident.

Debrief: What do we need to change for the future? Staff training, Online safety teaching, Parental Engagement, Review procedures and policies, Review of the filtering provision

Appendix K – Online safety advisory incident flowchart