St Mary Magdalen's Catholic Primary School

Online Safety Policy

Governors' Committee Responsible:	Full Governing Board
Status:	Non-statutory
Review Cycle:	Every two years
Date Written/Last Review:	23 June 2022
Date of Next Review:	22 June 2024

MISSION STATEMENT

We are a Roman Catholic community, placing God at the centre of our lives. Christian values permeate every aspect of the school day. As a small friendly school, we aim to produce the warmth and intimacy of the family. We recognise each individual as special and loved by God, caring for one another and fostering love, trust and respect. When mistakes are made we recognise them as opportunities for learning and consequent reconciliation.

We aim to help all children fulfil their potential. We have high expectations of the children; we want them to do their best socially, personally, academically and spiritually.

We recognise each child's full entitlement to education. We value children's uniqueness and endeavour to nurture their potential. We strive to promote in them a sense of personal worth and self-confidence, as well as an awareness of their responsibilities to self and others.

Contents

1   Aims

Our school aims to:
- have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology;
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2   Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

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

The policy also takes into account the National Curriculum computing programmes of study.

3.   Roles and Responsibilities

3.1   The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The governor who oversees online safety is Liam O'Connell.

All governors will:
- ensure that they have read and understand this policy;
- agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 5).

3.2   The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3   The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) and deputies are set out in our Safeguarding and Child Protection Policy.

The DSL takes lead responsibility for online safety in school, in particular:
- supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- working with the Headteacher, ICT Manager and other staff, as necessary, to address any online safety issues or incidents
- ensuring that any online safety incidents are logged (see Appendix 6) and dealt with appropriately in line with this policy;
- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the School Behaviour Policy;
- updating and delivering staff training on online safety (Appendix 5 contains a self-audit for staff on online safety training needs);
- liaising with other agencies and/or external services if necessary;
- providing regular reports on online safety in school to the Headteacher and/or governing board.

This list is not intended to be exhaustive.

3.4   The ICT Manager (ClickOn IT London Ltd)

The ICT Manager is responsible for:
- putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- conducting a full security check and monitoring the school's ICT systems on a monthly basis;
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

3.5   All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers, are responsible for:
- maintaining an understanding of this policy;
- implementing this policy consistently;
- agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 4), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2);

- working with the DSL to ensure that any online safety incidents are logged (see Appendix 6) and dealt with appropriately in line with this policy;
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:
- notify a member of staff or the Headteacher of any concerns or queries regarding this policy;
- ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2).

Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 4).

4 Educating Pupils About Online Safety

Pupils will be taught about online safety as part of the curriculum.

In Key Stage 1, pupils will be taught to:
- use technology safely and respectfully, keeping personal information private;
- identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in Key Stage 2 will be taught to:
- use technology safely, respectfully and responsibly;
- recognise acceptable and unacceptable behaviour;
- identify a range of ways to report concerns about content and contact.

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5 Educating Parents about Online Safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online Safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6 Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the School Behaviour Policy).

6.2 Preventing and Addressing Cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class Teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 12 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:
- cause harm, and/or
- disrupt teaching, and/or
- break any of the school rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the Senior Leadership Team to decide whether they should:
- delete that material, or
- retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- report it to the Police.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7 Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1, 2, 3 and 4). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

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

More information is set out in the acceptable use agreements in appendices 1, 2, 3 and 4.

8   Pupils Using Mobile Devices in School

Pupils may bring mobile devices into school, but they must be left at the school office when the pupil arrives at school and picked up at the end of the school day. Pupils are not permitted to use them whilst on school premises or during trips organised by the school.

Any breach of the acceptable use agreement (see appendices 1 and 2) by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9   Staff Using Work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 4.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT Manager.

Work devices must be used solely for work activities.

10   Children and Online Safety Away from School

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Safeguarding and Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police.

Online teaching should follow the same principles as set out in the school's Code of Conduct.

St Mary Magdalen's Catholic Primary School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Below are some things to consider when delivering virtual lessons, especially where webcams are involved:

- no 1:1's, groups only;
- staff and children must wear suitable clothing, as should anyone else in the household;
- any computers used should be in appropriate areas, for example not in bedrooms, and the background should be blurred;
- the live class should be recorded so that, if any issues were to arise, the video can be reviewed;
- live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day;
- language must be professional and appropriate, including any family members in the background;
- staff must only use platforms provided by the school to communicate with pupils;
- staff should record the length, time, date and attendance of any sessions held.

11   How the School Will Respond to Issues of Misuse

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

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12   Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and Child Protection Policy.

13   Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 7.
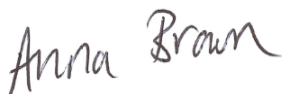
This policy will be reviewed every two years by the Premises Committee. At every review, the policy will be shared with the full governing board.

14   Links with Other Documentation

This Online Safety Policy is linked to our:
*   Safeguarding and Child Protection Policy;
*   School Behaviour Policy;
*   Staff Disciplinary Policy and Procedure;
*   Data Protection Policy and Privacy Notice;
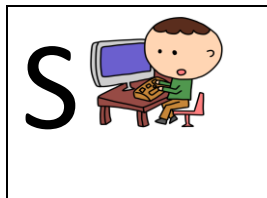*   Complaints Procedure.

Signed *Anna Brown*
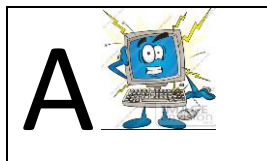
(for and on behalf of the Governing body)

Date 23/06/2022

St Mary Magdalen's Catholic Primary School

EYFS/KS1 Online Safety Agreement Form

S	I will only use the internet, computers and LearnPads with an adult present in the room
A	I will only click on icons and links when I know they are safe
F	I will only send friendly and polite messages
E	If I see something I don't like on a screen, I will always tell an adult

My Name:

Keeping safe: stop, think before you click!

St Mary Magdalen's Catholic Primary School

KS2 Rules for Keeping Safe Online

Keeping safe: stop, think, before you click!

These rules will keep everyone safe and help us to be fair to others.

I will only use the school's computers for schoolwork, clubs and homework.

I will only edit or delete my own files and not look at, or change, other people's files without their permission.

I will keep my logins and passwords secret.

I am aware that some websites and social networks have age restrictions and I should respect this.

I will not attempt to visit internet sites that I know to be banned by the school.

I will only use e-mail as directed by my teacher.

The messages I send, or information I upload or post, will always be polite and sensible.

I will not open an attachment, or download a file, unless I know and trust the person who has sent it.

I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.

I will never arrange to meet someone I have only ever previously met on the internet, unless my parent/carer has given me permission. I will take a responsible adult with me and meet in a public place.

If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher/responsible adult.

St Mary Magdalen's Catholic Primary School

KS2 Online Safety Agreement

Keeping safe: stop, think, before you click!

Pupil Name: _____

I have read the school 'rules for keeping safe online'. My teacher has explained them to me.

☐

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.

☐

This means I will use the computers, LearnPads, internet, e-mail, online communities, digital cameras, video recorders and other equipment in a safe and responsible way.

☐

I understand that the school can check my computer files, and the internet sites I visit, and that if they have concerns about my safety, that they may contact my parent/carer.

☐

Pupil's Signature: _____

Date: _____

Appendix 4: Acceptable Use Agreement (Parents/Carers)

St Mary Magdalen's Catholic Primary School

Parent/Carer Online Safety Agreement Form

Parent/Carer Name: _____

Pupil Name(s): _____

As the parent/carer of the above pupil(s) I grant permission for my daughter or son to have access to use the internet, and other computing facilities at school.

I know that my daughter or son has signed an online safety agreement form.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files, and the internet sites they visit, and that if they have concerns about their online safety or behaviour that they will contact me.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent/Carer Name: _____

Date: _____

Appendix 5: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

Acceptable Use of the School's ICT Systems and the Internet: Agreement for Staff, Governors, Volunteers and Visitors
Name of staff member/governor/volunteer/visitor:
When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: • access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature; • use them in any way which could harm the school's reputation; • access social networking sites or chat rooms; • use any improper language when communicating online, including in emails or other messaging services; • install any unauthorised software; • share my password with others or log in to the school's network using someone else's details.
• I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. • I agree that the school will monitor the websites I visit. • I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. • I will let the Designated Safeguarding Lead (DSL) and ICT Manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. • I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 6: Online Safety Training Needs – Self-Audit for staff

Online Safety Training Needs Audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreements for pupils and parents/carers?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Online Safety Incident Report Log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**