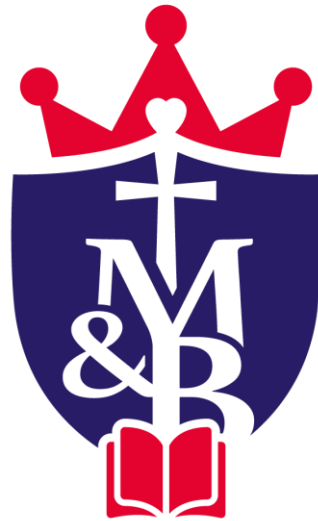


St. Mary's and St. Benedict's RC Primary School



St Mary's & St Benedict's RC Primary School

Online Safety Policy

'With Jesus, we learn as a joyful family and flourish to be the best that we can be.'

1. Introduction

The Headteacher, Governing Body and teaching staff of St Mary's & St Benedict's RC Primary School take their responsibilities for safeguarding pupils very seriously. We have a duty of care for child protection and we also strive to help parents to keep their own children safe and free from exploitation.

This policy works in conjunction with other school policies, particularly the Anti-Bullying Policy, Behaviour Policy and Safeguarding Policy. Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach.

2. Aims

Our school aims to:

- Outline and follow a clear policy to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which allows us to protect and educate the whole school community in its use of technology
- Establish a clear protocol to identify, intervene and escalate an incident, where necessary

3. Responsibilities

It is the responsibility of the entire school community to behave respectfully online and offline, and to use technology appropriately. To embed online safety successfully, this must also be modelled by all adults in school and parent/carers at home. It is the duty of all members of our school community to immediately report any concerns or inappropriate behaviour in order to protect pupils, families, staff and our school.

3a. Responsibilities: Staff and volunteers

All staff, including 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
- Ensuring all children in their care are supported to understand and follow the terms of acceptable technology use in our school
- Working with the DSL to ensure that any online safety incidents are reported, recorded and dealt with appropriately

3b. Responsibilities: Children

All children in our school have the right to be respected, heard and supported. In terms of online safety, they too have responsibilities to ensure this policy can be implemented successfully.

It is the responsibility of the children in our school to:

- Understand the importance of reporting abuse, misuse or access to inappropriate online materials
- Know what to do and who to talk to if they or someone they know feels worried when using online technology
- To understand and follow our school guidelines '12 rules for responsible ICT use'.

4. School Support

The school employs a dedicated technician for half a day each week from Lancashire Digital Education Services. Support focuses on ensuring effective maintenance of school resources, staff support and upkeep of our computer network.

5. Educating pupils about online safety

At St Mary's and St Benedict's, we adopt a whole school approach to online safety. To embed this policy, we maximise all cross-curricular links with Computing, ensuring that ample discussion and modelling is given to safe and effective use of technology.

In line with the National Curriculum for Computing, children at our school are taught key objectives at age appropriate levels. Within this teaching, children cover the following objectives for online safety:

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

In **Key Stage 2**, pupils 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

Throughout the school, the most notable links with online safety can be found within the following subjects:

- PSHE
- Relationships education, relationships and sex education (RSE) and health

- Computing
- Citizenship

6. Purple Mash

As a school, we have chosen the Purple Mash Computing scheme as it supports our teachers in delivering fun and engaging lessons, which help to raise computing standards and allow all pupils to achieve their full potential.

The implementation of Computing units in the PurpleMash programme will ensure a continuity and progression of skills, knowledge and understanding across the school. This is done by implementing computing skills in meaningful ways, and maximising cross-curricular links. Each Computing lesson embeds the principle of internet safety and looks to facilitate safe, responsible and respectful behaviour online.

Pupil to pupil messaging is not permitted in Key Stage 1 and is strictly controlled for the children in Key Stage 2. Messages require authorisation by staff before being sent/received, and children are continually reminded of the need for decency in their communications.

7. Acceptable use of the internet

We know that Computing can be a very exciting subject, yet at the same time we recognise that the use of these technologies can put young people at risk in and outside of the school. An 'Acceptable Use Agreement' has therefore been created to protect all parties. Parents, staff and children are expected to sign the agreements each year.

Two agreements have been created to support the needs of all children in our school. (EYFS/KS1 and KS2). (See Appendix A parts 1 and 2). Both agreements remind the children to ask trusted adults for advice and highlight the dangers of the internet in an age appropriate way.

As a school, we highlight a 12 step process for responsible ICT use, which is followed by staff and children alike. The rules are underpinned by the tag-line 'Stay safe: Think before you click', and are visible from every computer in our school. (See Appendix B).

When appropriate, the school will provide supervised access to internet resources. Access to streaming sites and inappropriate websites is strictly prohibited on our school network. This is managed by our ICT support (Lewis Loughborough).

Staff will preview any recommended sites before use.

If internet research is set for homework, specific sites must be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

6a. Online Safeguarding

St May's and St Benedict's subscribe to Netsweeper through Education Digital Services (formerly BT Lancashire Services). Netsweeper is an internet filter that is used to block inappropriate websites, and links to our school Safeguarding Policy. Netsweeper allows us to protect internet users against harmful websites through monitoring, reporting and filtering content across all devices. In the event that any staff witness or overhear use of inappropriate sites that remain accessible in school, it is their responsibility to inform the subject lead. The website, game or link will then be added to our 'blocked list' by our ICT Support lead (Lancashire Digital Education Services). The designated safeguarding lead (DSL) will also be informed.

7. Cyber bullying

Cyber bullying is bullying or intimidation which is carried out using electronic devices. BullyingUK define it as 'any form of bullying which takes place online or through smartphones and tablets'. Like other forms of bullying, it is the repetitive, intentional harming of one person or group.

7a.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 work with pupils to understand how they can report any incidents and are encouraged to do so. We also support them to report occasions 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.

In relation to a specific incident of cyber-bullying, staff will deal with this by following the processes set out in the school behaviour policy.

8. Safer Internet Day

Our whole school approach to online safety is further supported by Safer Internet Day, which takes place each year. Children learn how to stay safe on the internet and are taught how to recognise any dangers. Useful information is also shared to remind children of what to do and who to talk to if they witness, or are victims of bullying online.

9. Promoting online safety: Staff training

Online safety awareness is heavily linked with our school safeguarding policy. All school staff are 'Safeguarding Level 1 and 2' trained (completed September 2020).

In January 2021, all school staff completed an online course titled 'Online Safety- Risks to Children'. The course explored common misconceptions, potential dangers to children and shared guidance, legislation and management of such events in and outside of school. Upon completion, staff received an electronic certificate which are stored by the Computing subject lead (JV).

10.Home Learning

During home learning, or periods of individual isolation, Purple Mash and our school website are integral in supporting effective and quality learning at home. For further information, please see our remote/blended learning policy.

11.Password security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone and are changed when prompted. Staff must not leave a workstation having access to personal data unattended without locking the workstation or logging off from the network/machine.

Children are regularly reminded of the importance of keeping login details (e.g. Purple Mash) private.

12.Mobile phones: Staff, volunteers and other adults (including parents/carers)

The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device. The school is not responsible for the loss, damage or theft of any personal mobile device. The sending of inappropriate text messages between any members of the school community is not allowed.

Users bringing personal devices onto school premises must ensure there is no inappropriate or illegal content on the device.

Parents are reminded that no images are to be taken or shared during school events.

11a.Mobile phones: Children

The use of mobile phones and other digital devices by pupils in school is not permitted. Pupils in Year 5 and 6, who do bring phones into school, do so at their own risk. The device is locked in a filing cupboard for the day and returned to the child at the end of the school day.

13.Publishing images

No images or video will ever be shared without consent in our school.

When children join St Mary's and St Benedict's, their parent/carer will be asked to give permission to use their child's work/photos. Staff are informed accordingly of decisions with this matter. It is the responsibility of the parent/carer to inform the school of any changes to their decision.

14. Safe use of images and film

Digital images are easy to capture, reproduce and publish and therefore misuse. All staff must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking explicit consent and considering the appropriateness. With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils.

Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of themselves or others. This includes occasions in school and when on school trips

15. Inappropriate material

Accidental access to inappropriate materials must be immediately reported to the Headteacher/DSL.

Deliberate access to inappropriate materials by any user (adult or child), will lead to:

- The incident being logged by the Headteacher/DSL
- Full investigation by the Headteacher/LA and appropriate action taken.

Users are made aware of sanctions relating to misuse or misconduct. All staff are aware of the policy and the children and their parent/carer have signed an 'Acceptable Use Agreement'.

For further information, please see our 'What to do if...' document which outlines the guidelines to follow in the event of inappropriate ICT use within school. (Appendix C).

16. Complaints

Complaints relating to online safety should be made to the Headteacher/DSL and will be reported and recorded accordingly.

17. Parents and carers

We believe that it is essential for parents/carers to be fully involved with promoting online safety both in and outside of school. We regularly consult and discuss online safety with parents/carers, and seek to promote a wide understanding of the benefits related to IT and associated risks.

At St Mary's and St Benedict's, we raise parental/carer awareness of internet safety in letters and in information via our website and school app. We share information on how to be aware of social media and internet dangers. This includes information on apps such as TikTok and Houseparty, websites such as Instagram and Facebook and communication and streaming sites including Zoom and Netflix.

As part of our school Computing policy, parents and children are required to sign an 'Acceptable Use Agreement', highlighting that they have read and understood our rules for safe and appropriate use of ICT within school.

The 'Parents Acceptable Use Agreement' outlines their key responsibilities in relation to:

- Internet and IT
- Use of digital images, photography and video
- Social networking and media sites

If a parent or carer has any concerns, questions or queries about online safety, these can be raised with any member of staff or the headteacher (DSL).

Parents can seek further help and support on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre <https://www.saferinternet.org.uk/>
- Hot topics - Childnet International- <https://www.childnet.com/>
- Parent factsheet - Childnet International - <https://www.childnet.com/>
- National Bullying Helpline- <https://www.nationalbullyinghelpline.co.uk/social-media.html>
- BullyingUK- <https://www.bullying.co.uk/cyberbullying/what-is-cyberbullying/>

Subject lead: Jenni Venables

Date Written: December 2021

Reviewed: September 2022

Appendix A

St. Mary's & St. Benedict's Catholic Primary School regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Safeguarding Policies. We attempt to ensure that all students have good access to digital technologies to support their teaching and learning and we expect all our students to agree to be responsible users to help keep everyone safe and to be fair to others.

The Pupil Acceptable Use Agreement is attached to this form for reference.

Parents Acceptable Use Agreement

Internet and IT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

- the Internet at school
- the school's chosen email system
- the school's online managed learning environment <<name of system>>
- IT facilities and equipment at the school.

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 takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I will not take and then share online, photographs, videos etc., about other children (or staff) at school events, without permission.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe and responsible use of the Internet, online services and digital technology at home. I will inform the school if I have any concerns.

My daughter / son name(s): _____

Parent / guardian signature: _____

Date: ____/____/____

EYFS/Key Stage 1: Acceptable Use Agreement

I keep **SAFE** online because ...



I **CHECK** it's OK to use a website / game / app.

I **ASK** for help if I get lost online.

I **THINK** before I click on things.

I **KNOW** online people are really strangers.

I am **RESPONSIBLE** so never share private information.

I am **KIND** and polite online.

I **TELL** a trusted adult if I am worried about anything.

My trusted adults are:

Teacher

My name:

Date signed:

Teacher

--

Appendix A (part 2)

St. Mary's & St. Benedict's Catholic Primary School regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Safeguarding Policies. We attempt to ensure that all students have good access to digital technologies to support their teaching and learning and we expect all our students to agree to be responsible users to help keep everyone safe and to be fair to others.

The Pupil Acceptable Use Agreement is attached to this form for reference.

Parents Acceptable Use Agreement

Internet and IT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

- the Internet at school
- the school's chosen email system
- the school's online managed learning environment <<name of system>>
- IT facilities and equipment at the school.

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 takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I will not take and then share online, photographs, videos etc., about other children (or staff) at school events, without permission.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe and responsible use of the Internet, online services and digital technology at home. I will inform the school if I have any concerns.

My daughter / son name(s): _____

Parent / guardian signature: _____

Date: ____/____/____

KS2 Pupil Online Acceptable Use Agreement

This agreement will help keep me safe and help me to be fair to others.

I am an online digital learner – I use the school's IT for schoolwork, homework and other activities approved by trusted adults.

I am a secure online learner - I keep my logins and passwords secret.

I am careful online - I think before I click on links and only download when I know it is safe or has been agreed by trusted adults.

I am guarded online - I only give out my full home address, phone number or other personal information that could be used to identify me or my family and friends when my trusted adults have agreed.

I am cautious online - I know that some websites and social networks have age restrictions and I respect this and I only visit internet sites that I know my trusted adults have agreed.

I am considerate online - I do not get involved with bullying or sharing inappropriate material.

I am respectful online – I do not respond to unkind or hurtful messages/comments and tell my trusted adults if I receive these.

I am responsible online – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed online or is being affected by things they see or hear online.

I am a creative digital learner online - I only edit or delete my own digital work and only use other people's work with their permission or where the work is shared through a Creative Commons licence.

I am a researcher online - I use safer search tools approved by my trusted adults and know to 'double check' all information I find online.

I communicate and collaborate online - with people I know and have met in real life or that a trusted adult has approved.

I am SMART online - I understand that unless I have met people in real life, an online person is actually a stranger. I may sometimes want to meet these strangers so I will always ask my trusted adults for advice.

I have read and understood this agreement.

I know who are my trusted adults are and agree to the above.

Signed: _____

Date: _____

Appendix B


12 rules for responsible ICT use

Stay Safe: 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 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 will not bring files into school without permission or upload inappropriate material to my workspace.
- 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 e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, 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/carers has given me permission and I take a responsible adult with me.
- 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.

Appendix C

	Name of School	St Mary's and St Benedict's RC Primary School
	Guidance review Date	November 2020
	Date of next Review	November 2021

Guidance: What to do if...?

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the headteacher/e- safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered (Report to: **BT Lancashire Services**).
4. Inform the LA if the filtering service is provided via an LA.

An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided via an LA.

An inappropriate website is accessed intentionally by a staff member.

1. Ensure all evidence is stored and logged
2. Refer to the acceptable use and staffing policy that was signed by the staff member, and apply disciplinary procedure.
3. Notify governing body.
4. Inform the school technicians and ensure the site is filtered if need be.
5. Inform the LA if the filtering service is provided via an LA.
6. In an extreme case where the material is of an illegal nature:
 - a. Contact the local police and follow their advice.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you; do not view the misuse alone.
2. Report the misuse immediately to the headteacher and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the headteacher should then:
 - Remove the device to a secure place.

- Instigate an audit of all ICT equipment by the schools ICT managed service providers or technical teams to ensure there is no risk of pupils accessing inappropriate materials in the school.
 - Identify the precise details of the material.
 - Take appropriate disciplinary action (undertaken by Headteacher).
 - Inform governors of the incident.
4. In an extremecasewhere the material is of an illegal nature:
- Contact the local police and follow their advice.
 - If requested to remove the device to a secure place and document what you have done.

All of the above incidences must be reported immediately to the head teacher and online-safety officer.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including online-safety, behaviour and PHSE, and apply appropriate sanctions.
3. Secure and preserve any evidence through screenshots and printouts.
4. Inform the sender's e-mail service provider if known.
5. Notify parents of all the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform other agencies if required (LA, Child protection)

Malicious or threatening comments are posted on an Internet site (such as social networking) about member of the school community (including pupils and staff).

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at www.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA and other agencies (child protection, Governing body etc).

The school may wish to consider delivering a parent workshop for the school community.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with the child.

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP <http://www.ceop.gov.uk/>
4. Consider the involvement police and social services.
5. Inform LA and other agencies.
6. Consider delivering a parent workshop for the school community.

You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the child.

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child and parents on appropriate games and content. You may want to use template letters to inform all or targeted parents.
3. If the game is played within school environment, ensure that the technical team block access to the game
4. Consider the involvement social services and child protection agencies.
5. Consider delivering a parent workshop for the school community.

You are aware of social network posts and pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.

1. Contact the poster or page creator and discuss the issues in person
2. Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
3. Contact governing body and parent association
4. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the headteacher and online-safety officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology and they must be able to do this without fear.