Online Safety Policy

St Mary Magdalen's C of E Primary School

At St Mary Magdalen's we believe that:

We must Inspire our children, and in order to do this we must:

- Promote Enjoyment;
- Strive for Happiness;
- Develop an environment where children are glad to come to school;
- Celebrate our successes;
- Always aim to have health and well-being.

By accepting God's word, Love will always be at the centre of our school and we will show this by:

- Remembering our uniqueness;
- Believing in equality and accepting and respecting differences;
- Living by our Christian values;
- Forging partnerships;
- Being Forgiving;
- Accepting forgiveness;
- Showing patience;
- Being prayerful;
- Ensuring there is a safe environment both physically and emotionally for our children and staff to grow in;
- Having self-reflection; • Remembering our spirituality;
- Creating a love of learning.

When we Educate our children, we must:

- Ensure that all our children achieve their full potential;
- Remember the whole child;
- Have high expectations in all areas for all our children;
- Create a curriculum to stimulate all our children.

Updated 17.10.22

Developing and Reviewing this Policy

This Online Safety Policy has been written as part of a consultation process involving the following people:

………

It has been approved by Governors and will be monitored and reviewed as listed below:

Policy Created - Date: ……………………………………

The implementation of this policy will be monitored by ………………………………………………..

This policy will be reviewed as appropriate by
……………………………………………………………………………………………..

Approved by …………………………………… (Headteacher) Date ………………………………………

Approved by …………………………………… (Governor) Date ………………………………………

Contents

Online Safety Policy Sept 2021 - St Mary Magdalen's CE Primary School

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our Online Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

2. Our school vision for Online Safety

Updated 17.10.22

At St. Mary Magdalen's we use technology when appropriate to enhance the learning experience for our children and to support the daily organisation and administration tasks carried out by our staff.

Keeping members of our school community safe whilst using technology is a priority and we expect staff to act as role models in their use of technology and abide by the shared decisions reflected in our Online Safety policy. Children are encouraged to explore and make responsible decisions regarding their uses of technology, informed by 'education' as opposed to the imposition of restrictions. As children are engaging with 21st Century technologies both inside and outside of school, we will provide opportunities for both children and the wider community to understand and view Online Safety education as a key life skill.

Our Online Safety Policy defines what we consider to be acceptable and unacceptable behaviour regarding the uses of technology in our school and the sanctions or procedures to be followed should breaches of security occur. It is communicated to staff, pupils and committee members and is updated in light of the introduction of new technologies or incidents.

3. The role of our school Online Safety Champion

The Online Safety Champion is a nominated point of contact within school for Online Safety related issues and incidents. Certain responsibilities may need to be delegated to other staff e.g. Designated Senior Person/Child Protection Officer as is necessary.

Our Online Safety Champion is: **Mr Gary McNab**

The role of the e Safety Champion in our school includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school Online Safety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Ensuring the e Safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with Online Safety issues and guidance through liaison with the Local Authority Schools'' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging Online Safety advice/training for staff, parents/carers and governors.

- Ensuring the staff, pupils and committee members are updated as necessary.
- Liaising closely with the school's Designated Senior Person / Safeguarding Officer to ensure a co-ordinated approach across relevant safeguarding areas.
- Where necessary, to contact outside agencies if a breach of security or Online Safety incident occurs, eg the police or CEOP.

4. Policies and practices

This Online Safety policy should be read in conjunction with the following other related policies and documents:

- School Self Evaluation Framework
- Improvement Plan
- Staff Code of Conduct, Recruitment and Induction Procedures
- Anti-Bullying Policy
- Behaviour Policy
- Safeguarding Policy

4.1 Security and data management

In order to protect children, staff, committee members and other members of the school community our data is kept secure and all staff are informed as to what they can / cannot do with regard to data in the following ways:

- The Online Safety champion has overall responsibility for managing all information.
- Staff have been informed of the location of all data relevant to them by the Online Safety champion.
- Staff have been informed of their legal responsibilities with respect to principles of the Data Protection Act (2018) and ensure all data is :
    1. Accurate
    2. Secure
    3. Fairly and lawfully processed
    4. Processed for limited purposes
    5. Processed in accordance with the data subject's rights
    6. Adequate, relevant and not excessive

7. Kept no longer than necessary

8. Only transferred to others with adequate protection

Our school ensures that data is appropriately managed both within and outside the school in the following ways:

Equipment, including Computers, I pads , laptops, cameras and storage devices must only be used for school purposes and not contain personal information eg, personal images, personal financial details, music downloads, personal software.

- Computers are accessed via a username and password and it is the responsibility of the individual to keep this secure at all times. Passwords must not be written down, unless they are securely stored, eg in a safe. Any breaches in security must be reported immediately to the Online Safety champion.

- School equipment must not be used, for example, for online gambling, dating websites home shopping, booking holidays and social networking BOTH at home and in school.

- Online Safety champion is responsible for disposing of sensitive data, eg, shredding hard copies, deleting digital information.

  School data must NOT be stored on personal equipment, eg, home computer or mobile phone, this includes images, photos, reports, and test results.

Updated

17.10.22•

Staff are not allowed to use personal storage devices, eg, external hard drives, pen drives, mobile phones on school equipment.

- Child protection data and other sensitive information should not be saved on mobile devices at all to avoid loss of the data.
- The school will ensure that children cannot access terrorist and extremist material when using the internet.
- The school will ensure that children cannot access inappropriate material when using the internet
- The school network which is backed up on a regular basis.

4.2 Use of mobile devices

We recognise the use of mobile devices offers a range of opportunities to entertain and extend children's learning. However, the following statements must be considered when using these devices

- Children must not use their own mobile devices in school as these could potentially circumvent the **NET SWEEPER** filtering system and other security systems within this policy.
- Children should not be permitted to use staff mobile devices.
- Mobile devices brought into school by children must be kept turned off and handed into the school office until taken home.
- mobile devices should be used in accordance with the rest of this policy.
- mobile phones should only be used by staff in accordance with the Acceptable Use policy.

  Staff mobile phones should not be used during sessions. (see later points in 4.4mobile phones)
- Mobile devices brought onto the school premises are done so entirely at the owners' risk.
- Non-school mobile devices will not be permitted to access the school network and must not hold any school data.
- Non-school mobile devices must not be used for taking or storing images, video or audio recordings of pupils.

4.3 Use of digital media

Updated

17.10.22•

We are aware of the issues surrounding the use of digital media online. All STAFF members understand these issues and need to follow the guidance below.

Permission is sought from parents/carers to take and use their child's photograph for school purposes. This includes but is not limited to: use on the school website, use in newspapers, the school prospectus and for displays within the school building.

- Permission is also sought to keep these images after a child has left the school. This covers the same usage sought above.
- Where an image is used, no other personal information about the child will be given, including their name.
- Only a child's first name will appear on any digital media, unless additional parental consent has been given, eg in a newspaper article.
- Parents/carers must not take photographs of children in the school as this may include children other than their own.
- Digital media including pupils should not be posted by staff on personal social networking sites.
- Only school equipment should be used for recording images, video and audio of pupils. This must only be done for school purposes.
- Photographs, video and audio of pupils must only be stored on the network.
- Digital media must not be stored on staff's personal equipment.
- When taking images and video staff must ensure that subjects are appropriately dressed and not taking part in activities that could be misinterpreted.

Pupils, staff, parent/carers and other adults in school will be made aware of the dangers of publishing images and videos of pupils or adults on social networking sites or websites without the consent of the persons involved. This will be done at the same time as consent is sought for internet and photo permissions.

4.4 Communication technologies Email:

The following statements reflect our practice in the use of email.

- All staff have access to the **Lancashire Digital Education Service**.
- Only official Microsoft Office/Lancashire Digital Education Service email addresses should be used to contact staff, pupils, parents and outside agencies.

Updated

17.10.22•

- Lancashire Digital Education Service email accounts should only be used for school related communication, ie nonpersonal use.

  NETSWEEPER filtering service should reduce the amount of SPAM (Junk Mail) received on Lancashire email accounts. However, any incidents of SPAM should be reported to the **Lancashire Digital Education Service** by the Safety champion to support this.

- Staff are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, and will not access these in school.

- All users are aware that email is covered by Data Protection Act (2018) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.

- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.

- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

- Staff will include a standard disclaimer at the bottom of all outgoing emails.

E-mail disclaimer:

This e-mail and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent St. Mary Magdalen's CE Primary School. If you are not the intended recipient, you must not use, disseminate, forward, print or copy this e-mail or its contents. If you have received this e-mail in error, please contact the sender. Please note that e-mail may be monitored in accordance with both school policy and the telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.

Social Networks:

Many adults and pupils regularly use Social Network sites, e.g. Instagram, Snapchat, Facebook or Twitter, although the minimum age for registering for some of these excludes primary school pupils. These communication tools are, by default, 'blocked' through the internet filtering system for direct use in Lancashire schools. However, comments made outside school on these sites may contravene confidentiality or bring the school or staff into disrepute.

Updated

17.10.22•

In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

All staff need to be aware of the following points:

They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.

- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum.
- Pupils must not be added as "friends" on any Social Network site.
- Remember; whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Staff will also be given additional guidance from county on social networking sites as it becomes available (by Online-Safety champion).

Mobile telephone:

In our school the following statements outline what we consider to be acceptable and unacceptable use of mobile telephones:

NB: these guidelines are for the use of phones for communication only – photos and storage are covered elsewhere.

- Staff and visitors may only use personal mobile phones outside of session times unless absolutely necessary, eg in an emergency.
- Children must not use their own mobile phones in school.
- Children should not use staff personal mobile phones unless absolutely necessary, eg staff injury.

Instant Messaging:

The following statements outline what we consider to be acceptable and unacceptable use of Instant Messaging:

Instant messaging will not be used by anyone in school unless it is:

- Internally hosted or externally ie: Purple Mash

Updated

17.10.22•

- No school equipment should be used outside of school for instant messaging

  purposes.

Web sites and other online publications

The following statements outline what we consider to be acceptable and unacceptable use of websites and other online publications:

- Staff who upload images, text, etc to the website will be made aware of the guidance for digital images (section 4.3).
- Children may be mentioned on the website by the use of their first name only. This will not be accompanied by an image of them. An image may only be used with permission of the child's parent/carer. No other personal information about children will be uploaded.
- Materials will only be placed on the website which do not infringe upon copyright/persona; intellectual copyright restrictions.
- Staff are aware that anyone can access the website.
- Documents on the website should be in a read-only format (.pdf) to help prevent content being manipulated and potentially redistributed without the school's consent.

Others:

This policy will be updated and amended as necessary when new technologies become available.

4.5 Acceptable Use Policy (AUP)

- Acceptable Use Policies will be in place which reflect the technologies, procedures and practice within our school and will be reviewed when this policy is amended and updated as necessary.
- These Acceptable Use Policies will be signed by parents, staff, and children.
- See the AUPs at the end of this document.

4.6 Dealing with incidents

An incident log, kept in the server room will need to be completed by a relevant member of staff should an e Safety issue occur. This log book will be audited by the e Safety Champion.

Illegal Offences

- Any suspected illegal material or activity will be brought to the immediate attention of Online Safety champion who will refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF - https://www.iwf.org.uk/).

- **Staff must never personally investigate, interfere with or share evidence as they may inadvertently commit an illegal offence.**

- It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident (see guidance within this document on correct procedures).

- The Online Safety Champion will immediately report potential illegal content to the Internet Watch Foundation (https://www.iwf.org.uk/).The IWF are licensed to investigate – schools and schools are not.

Updated 17.10.22

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

More details regarding these categories can be found on the IWF website (http://www.iwf.org.uk).

Inappropriate use

Incident	Procedure and Sanctions
Accidental access to inappropriate materials.	Minimise the webpage/turn the monitor off. Tell an adult. Adult to enter the details in the Incident Log and inform Online Safety Champion. Online Safety Champion to report to LGfL filtering services if necessary. Persistent 'accidental' offenders may need further disciplinary action in line with the behaviour policy.
Using other people's logins and passwords maliciously. Deliberate searching for inappropriate materials.	Inform Online Safety Champion. Enter the details in the Incident Log. Additional awareness raising of Online Safety issues and the AUP with child. More serious or persistent offences may result in further disciplinary action in line with the behaviour policy. Consider parent/carer involvement.
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

- The supervising adult is immediately responsible for dealing with Online Safety incidents and for recording them in the log book. It may be necessary to escalate the incident to another member of staff. This may include the manager or Online Safety Champion.

- All staff are aware of the different types of Online Safety incident, e.g. illegal or inappropriate.
- All staff are aware of the procedures to follow if an Online Safety incident occurs.
- An outline of procedures to follow to be kept in the log book.
- Children are informed of the procedures during Online Safety sessions, posters in the ICT suite and as necessary.
- All Online Safety incidents are to be recorded as soon as possible in the incident log book.

  The log book is monitored by the Online Safety Champion once per term.
- External agencies will be contacted immediately for illegal or severe incidents.
- Parents will be notified if their children are 'repeat offenders' or if an illegal or severe incident occurs.
- Children who break the AUP rules will be subject to normal behaviour expectations sanctions.
- Children who repeatedly cause Online Safety incidents may be banned from using such equipment for a period of time, depending on the offences and at the Online Safety champion's discretion.

5. Infrastructure and technology **Pupil Access:**

- Pupils will be supervised by an adult when they access online materials.

Passwords:

- Staff to be aware of the relevant guidelines in the ICT Security Framework.
- Staff have secure passwords to access the school network.
- Passwords must not be written down, unless they are securely locked away.
- Staff passwords should be aware that strong passwords:

  ○ Are at least 6 characters in length; ○ Contain a combination of numbers, symbols lowercase and uppercase letters, ○ Should not be easy to guess, eg don't use the name of your pet.

- Children log on to the network using class credentials to ensure they can all access the computers within a reasonable amount of time.

- The admin password for servers is only known by the Online Safety champion and the necessary SLT staff. The admin password is changed every 12 months

- Staff are aware that they are responsible for the security of their password. They acknowledge that they may be held responsible for any actions which take place whilst the network is accessed with their credentials.

Software/hardware:

- Licences for all software will be managed by the school.

Managing the network and technical support:

- Users must not try to circumvent security measures put in place on equipment.

- If any user suspects a break in security then they should ensure the computer is no longer used and contact Mr McNab as soon as possible.

- Removable storage devices should not be used on the network or on school equipment.

- Users should not use data CDs or DVDs they have 'burnt' themselves on school equipment.

- School equipment (including, but not limited to, laptops, cameras and netbooks) must not be used for personal/family use; they should only be used for work purposes.

- No-one should be allowed to use staff laptops apart from the member of staff it is allocated to.

- Network monitoring will take place in accordance with the Data Protection Act (2018)

- Mr McNab is responsible for keeping logs and monitoring use of the school network and related equipment.

- Staff will be made aware of the network use which is logged and monitored. This may include but is not limited to: login dates and times, the computer that is used, websites visited, images viewed, files downloaded Printer usage, programs used and similar information.

- Any breeches in this policy, and accompanying Acceptable Use Policies, by pupils, staff and other users will be reported to the Online Safety champion and appropriate action will be taken as appropriate, eg disciplinary action and/or involving external agencies if necessary.

Filtering and virus protection:

- The school has devolved control over the Netsweeper filtering service.
- The filtering is managed by The Headteachers and GMC.

If staff suspect a computer or laptop has been infected with a virus they should report it immediately GMC

6. Education and Training

6.1 Online Safety across the curriculum

□ • Children will be made aware of relevant Online Safety rules by the school. And details how we keep pupils safe when using the internet and mobile technology

6.2 Online Safety – Raising staff awareness

- Advice/guidance may be given to individuals at any time by Online Safety champion.
- Online Safety champion to seek updates from CEOP and county prior to Online Safety training sessions and throughout the year.
- Online Safety champion to give updates to staff on Online Safety policy, AUPs and general Online Safety issues as required.
- During training sessions staff are to be made aware of issues which may affect their own personal safeguarding, eg use of social networking sites and forums.

6.3 Online Safety – Raising parents/carers awareness

□ The school will raise awareness and promote suitable external Online Safety resources as and when they become available.

7. Standards and inspection

- Online Safety incidents are monitored and reviewed by the Online Safety Champion once per term.
- Online Safety incidents will be recorded by the member of staff dealing with the incident as soon as possible in the Online Safety incident log book.

Updated 17.10.22

- New technologies are to be considered in light of the e Safety policy, which will be updated if necessary to accommodate the use of such technology in the school.

- When monitoring Online Safety incidents in the log book, the Online Safety Champion will check to see if there are recurring patterns based on eg, specific days, times, classes, groups and individual children.

- If any patterns are found, the Online Safety Champion will decide on how best to address the issues raised, eg working with specific groups or children, assemblies or reminders to parents.

- Any Online Safety issues discovered through the reporting and monitoring of Online Safety incidents, where necessary, lead to appropriate changes in the Online Safety policy and practice.

- Acceptable Use Policies will take into account current trends and new technology as it emerges.

- Staff will be made aware of changes to the policy by Online Safety champion.

APPENDIX 4 ICT Acceptable Use Policy (AUP) – Parent's Letter

Dear Parent/Carer,

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

This is particularly relevant when using Social Network Sites which are becoming increasingly popular amongst both the adult population and young people. However, many sites do have age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of these age-restriction policies and therefore we actively discourage this in our school.

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

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible.

Along with addressing Online Safety as part of your child's learning, we will also be holding Parental e Safety Awareness Sessions during the school year and I would take this opportunity to strongly encourage your attendance wherever possible. Further information on these sessions will be communicated as soon as dates are confirmed. In the meantime, if you would like to find out more about Online Safety for parents and carers, please visit the https://www.thinkuknow.co.uk/parents/Listing/?cat=66,67,68,69,70,72&ref=4765&keyWord=&p=1 Also, there are links on the school website.

Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguards the pupils in school.

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

APPENDIX 1 Classroom Online Safety (EYFS/KS1)

Our Golden Rules for Staying Safe with ICT EYFS/KS1

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

We are always polite and friendly when using online tools.

We always make careful choices when we use the Internet.

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

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

APPENDIX 2 Typical Classroom Online Safety (KS2)

Our Golden Rules for Staying Safe with ICT KS2

We always ask permission before using the internet.

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

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

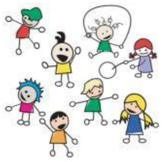
We only communicate online with people a trusted adult has approved.

All our online communications are polite and friendly.

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

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

Inspire Love



Educate

Reaching our potential together in Christ .

APPENDIX 3 Parental Online Safety Awareness Session

Dear Parent/Carer,

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

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

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

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

Date: ________________________________Time___________________________________

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

What are our children doing online and are they safe?
Do they know what to do if they come across something suspicious?

Are they accessing age-appropriate content? How can I help my child stay safe online?

The session will last for approximately 1¼ hrs where a member of the Local Authority Schools' ICT Team will present an Internet Safety session to address the issues mentioned above.

Yours sincerely,

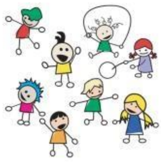
Mrs Karen Hardman and Mrs Helen Bird

Inspire

MM

St Mary Magdalen's

Love



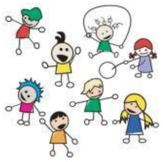
Educate

Reaching our potential together in Christ .

I / we will be attending the above Parental Online Safety Awareness Session

*Name(s):*____

Parent / Carer of: _________________________________ *Year Group* __________



APPENDIX 4 – Online Safety Incident Log

All Online Safety incidents must be recorded by the person involved or School Online Safety Champion. This incident log will be monitored and reviewed regularly by the Online Safety Champion.

Any incidents involving Online bullying should also be recorded on the 'Integrated Bullying and Racist Incident Record Form 2' available via the Lancashire Schools' Portal.

Date / Time of Incident	Type of Incident	Name of pupil/s and staff involved	System details	Incident details	Resulting actions taken and by whom (and signed)