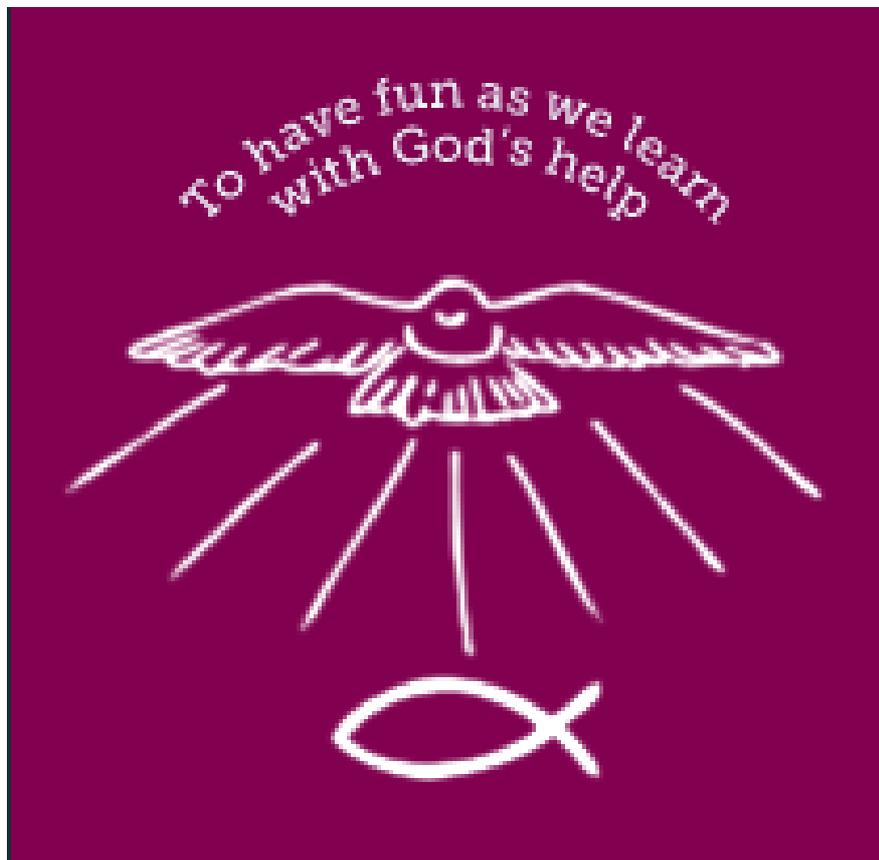


St Margaret Clitherow
Catholic Primary School



E-Safety Policy

September 2021

OUR MISSION STATEMENT

Our Mission is to provide a Catholic education based on the life and teaching of Jesus Christ, in which the values of the Gospel underpin all aspects of school life. We insist on the highest standards of academic achievement so that our young people leave us as ‘agents of change’ – educated and caring people who have the qualifications, knowledge and skills they need to flourish as human beings and make the world a better place. We are committed to our mission and to raising standards in order to provide an excellent Catholic education for every child in our care. We work together as one Trust, one family of schools, a community inspired by a vision for excellence.

We aim to deliver our mission by:

- Promoting our **Core Gospel Values** which underpin all aspects of school life
- Promoting **stewardship** enabling our children to develop an understanding of the wider world and their role as global citizens
- Providing opportunities for our children to be **agents of change** and to make a positive difference to the world in which they live
- **Balancing academic success with wider attributes** & provides for learners broader development enabling them to **develop and discover their interests and talents**
- Promoting our **Learning Values** – resilience, responsibility, independence, creativity & collaboration
- Supporting our children to develop their **character** and help them to keep **physically and mentally healthy**
- Placing an uncompromising focus on the development and application of **reading, writing and mathematics skills**
- Playing a major role in developing our children’s **love and passion for learning**
- Celebrating **equity and diversity** supporting the pupils’ spiritual, moral, social and cultural development
- Developing **children as leaders** by valuing children’s voices and individual contributions and offering a range of opportunities to develop their leadership skills

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors..

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents (*insert others appropriate to your own school needs*).

Safeguarding is a serious matter; at St Margaret Clitherow Catholic Primary School, we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on our school website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Pupils' Acceptable Use Policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to school technology including the Internet.

Headteacher Name:

Signed:

Chair of Governors:

Signed:

Review Date: September 2021

Next Review: September 2022

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have responsibility for the governance of e-safety at the school (under the umbrella of Safeguarding) who will:
 - Keep up to date with emerging risks and threats through technology use.
 - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.
- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly
- Advise the governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with CAST and IT Technical Support.

IT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
 - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
 - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
 - Any e-safety technical solutions such as Internet filtering are operating correctly.

- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
- Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters. Pupil passwords are changed annually.
- Two-Step validation is in place and used by all staff.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident is reported to the Headteacher (and an e-Safety Incident report is made).
- The reporting flowcharts contained within this e-safety policy are fully understood.
- Two-step validation is in place.

All Pupils

The boundaries of use of IT equipment and services in this school are given in the Pupil Acceptable Use Policy; any deviation or misuse of IT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings and school newsletters, the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the Pupil Acceptable Use Policy before any access can be granted to school IT equipment or services.

Technology

St Margaret Clitherow Catholic Primary School uses a range of devices including PCs, laptops, Chrome Books and tablets. In order to safeguard the pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use SWGFL software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an

incident, whichever is sooner. The Headteacher and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are resolved.

Email Filtering – we use Google Mail software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the Trust to ascertain whether a report needs to be made to the Information Commissioner's Office. *(Note: Encryption does not mean password protected.)*

Passwords – all staff and students will be unable to access any device without a unique username and password. Staff and pupil passwords termly/annually or if there has been a compromise, whichever is sooner. The Headteacher and IT Support will be responsible for ensuring that passwords are changed.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as keydrives are scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy. Letter explaining filtering and monitoring of the internet is sent home annually.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Students are permitted to use the school email system, and as such will be given their own email address. The email address will be made up of their first initial and surname, e.g. jsmith@smcprimary.org

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; St Margaret Clitherow Catholic Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within St Margaret Clitherow Catholic Primary School and have been appropriately risk assessed; should staff wish to use other social media, permission

must first be sought from the Headteacher. Any new service will be risk assessed before use is permitted.

- Blogging
- Twitter
- Facebook

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupils using first name and surname; first name only is to be used.
- Where services are “comment enabled”, comments are to be set to “moderated”.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner’s permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any e-safety incident is to be brought to the immediate attention of the the Headteacher and the incident logged.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, St Margaret Clitherow Catholic Primary School will have an annual programme of training which is suitable to the audience.

E-Safety for pupils is embedded into the curriculum; whenever IT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student’s learning. Specific e-safety lessons for pupils will be taught as a minimum at the start of each half term.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Education Offsite Covid19 Pandemic - Due to the current Covid19 pandemic, it must be recognised that there may be incidents where individual children, groups of children or the whole school may be required to work from home and will need to access online learning through a non-filtered and monitored device. Therefore, during these times, the teaching of online safety is even more fundamental and must be at the forefront of the 2021/2022 curriculum.

Where a child or group of children are working from home, they may be asked to access learning via online video meetings through services such as Zoom. Staff and children must adhere to the

protocols set in place by the school for these meetings and where these protocols are broken this must be reported to the DSL.

Staff protocols for online video meeting-

- Date and time of chat only shared in secure email
- Link to chat only shared in secure email
- Staff to set up Zoom accounts using their professional email address
- Only conversations instigated by staff member to be undertaken.
- Participant to wait in waiting room until admitted by teacher.
- Videos must be on for all participants and correct name used, otherwise they will be removed from the online meeting.
- Where possible all online meetings will be recorded through zoom and saved onto the teachers computer.
- Staff must learn what features there are and what you must do and what are optional e.g use [tutorials](#). Teachers must learn how to lock and record the online meeting, prevent other users from sharing their screen, place pupils on hold, disable and mute microphones and videos.
- School laptops/iPads are the only equipment which can be used to stream Zoom sessions with class/pupils
- Staff to, when possible, make calls whilst in school and that meetings are held in a communal area.
- If calls have to be made from a staff members home, staff to ensure that background area is free from personal items like family photographs, links to address.
- Staff must ensure they only enable known users into conversations.
- Ensure professional dress and conversation at all times.
- Permission for meeting to be gained by parents by sending invite to parent's email.

Child/Parent protocols for online video meeting-

- Parents to be aware of school guidance.
- An adult must be present in the same room as the child joining the online meeting.
- Child must be in a room where the background will not cause offence or be inappropriate to anyone else in the chat.
- Children to be reminded to act respectfully and only use chat for appropriate messages.

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both you must sign this policy sheet (*it may be easier and tidier to have a separate single sheet that all staff sign*).

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the e-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become “friends” with parents or pupils on personal social networks

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support.

Viruses and other malware - any virus outbreaks are to be reported to the Headteacher as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

e-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of IT whether you are with other members of staff or with students.

NAME :

SIGNATURE :

DATE :

Acceptable Use Policy – Students

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people’s work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people’s usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online ; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent) :

Signed (Student) :

Date :

Letter to Parents

Dear Parent/Guardian

Use of the Internet in school is a vital part of the education of your son/daughter. Our school makes extensive use of the Internet in order to enhance their learning and provide facilities for research, collaboration and communication.

You will be aware that the Internet is host to a great many illegal and inappropriate websites, and as such we will ensure as far as possible that your child is unable to access sites such as this. We are able to do this using advanced software known as an Internet filter. This filter categorizes websites in accordance with their content; the school allows or denies these categories dependent upon the age of the child.

The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school; in order to ensure that there have been no attempts of inappropriate Internet activity we may occasionally monitor these logs. If we believe there has been questionable activity involving your child we will inform you of the circumstances.

At the beginning of each school year we explain the importance of Internet filtering to your child. Furthermore we explain that there has to be a balance of privacy and safety; we also inform them that we can monitor their activity. All children are given the opportunity to ask questions and give their viewpoint. We would like to extend that opportunity to you also; if you have any questions or concerns please contact admin@smcprimary.org

Yours Sincerely

C Lowry
Interim Executive Headteacher

I have read this letter and understand that my child's Internet access could be monitored to ensure that there is no illegal or inappropriate activity by any user of the school network. I acknowledge that this has been explained to my child and that he/she has had the opportunity to voice their opinion, and to ask questions.

Name of Parent/Guardian:

Name of Child:

Signature:

Date