The Royal Borough of Kingston upon Thames

Malden Parochial C of E Primary School

Online Safety Policy

Agreed : Autumn term 2020
Review date : Autumn term 2022
[or as required]

MALDEN PAROCHIAL C OF E SCHOOL

Ethos Statement

This is a Church of England Primary School. As such, its ethos derives from the Christian Gospel. In all that it does or aspires to achieve, the school is informed and strengthened by Christian belief and practice.

At the heart of the school's ethos is the conviction that God loves each person: that God desires the best for each person; that God longs for each person to develop their potential as human beings.

Mission Statement

In accordance with the Ethos Statement, our school will aim to provide high quality education to the children of the local community within a safe, happy and stimulating environment

Love, Learn, Live!

Contents

Opening statement

Teaching and learning

Managing internet access

Policy Decisions

Communication

Concluding statement

Appendices

Appendix 1 – Online safety scheme of work

Appendix 2 – Sample codes of conduct

Appendix 3 – Resources for parents/carers

Appendix 4 – Categories of Cyber bullying

Appendix 5 – Advice for pupils regarding Cyberbullying

Appendix 6 – Online safety advice for parents/carers

Opening statement

At Malden Parochial we believe that the internet is an essential resource in 21st century life for education, business and social interaction. We understand that computing plays an important role in our everyday lives and we accept our responsibility to teach our staff and pupils how to use the Internet safely.

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used.

This online Safety Policy recognises and seeks to develop the skills that children and young people need when communicating and using these technologies properly, alongside keeping safe and secure, and acting with respect for others.

This policy should be read in conjunction with other documents including Child Protection and Safeguarding Policy and Procedure, Anti-bullying Policy and Preventing Extremism Policy.

Teaching and Learning

Why the internet and digital communications are important

Developing effective practice in internet use for teaching and learning is essential. The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. To accomplish this staff and children will need access to:-

- World-wide educational resources including museums and art galleries
- Educational and cultural exchanges between pupils world-wide
- Vocational, social and leisure use in libraries, clubs and at home
- Access to experts in their fields for pupils and staff
- Staff professional development through access to national developments
- Communication and collaboration with support services and professional associations
- Improved access to technical support including remote management of networks
- Exchange of curriculum data with the Local Authority and Department of Education • Access to learning and information wherever and whenever convenient

Evaluating of Internet content

The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Security will include:

* Pupils being taught what internet use is acceptable and what is not and given clear objectives for internet use;

* Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of

pupils; * Staff should guide pupils during on-line activities to support the learning outcomes planned for the pupils' age and maturity;
*	Pupils will be given their own logins to the computers and access limitations to the	internet will have been set by the Subject Leader for Computing; and,	* Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Managing internet access

Security

The Subject leader for Computing/online safety is responsible for reviewing the IT system with regards to security with the support and advice from the local authority, CLICKonIT, LGFL, Atomwide and CEOP.

- School technology systems security will be reviewed on a regular basis
- Virus protection will be updated weekly with an up to date virus's protection software from Atomwide. (SOPHOS)
- Filtering of websites and email is refreshed everyday by ATOMWIDE. Any reported unsuitable websites are reported to the Subject Leader for Computing   who will arrange for this website to be blocked using a software package called WEBSENSE.
- The Subject Leader for Computing will audit filtering systems regularly with LGFL and Atomwide to continue promoting safety of the Internet for all users.
- School servers will located securely and physical access restricted. The server operating system will be secured and kept up to date.
- Access by wireless devices will be pro-actively managed.
- Firewalls and switches will be configured to prevent unauthorised access between schools. Personal data sent over the internet will be encrypted.
- Portable media will not be used without specific permission followed by a viruses check; unapproved system utilities and executable files will not be allowed in pupils work areas or attached to e-mail.
- Parents/carers are advised to use the school email address and telephone number as a point of contact. Information regarding individual members of staff or pupils will not be published.
- Written permissions is sought from parents/carers in regards to the use of photographs of their children, this includes our school website. In any situation where photographs are used the child's full name will not be published.

Emails

- Pupils may only use approved e-mail accounts supplied by the school Subject Leader for Computer which are monitored on a regular basis by LGFL and the Subject Leader.
- Pupils must immediately inform a teacher or member of staff if they receive an offensive email.
- In email communication, pupils will be taught not to reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming email should be treated as suspicious and attachments not opened unless the author/sender is known.

- Pupils will not be able to access personal email accounts (home accounts) due to blocking filters built into the school internet access.
- Emails sent to an external organisation will be written carefully and authorised before sending in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- The sending of abusive or inappropriate email messages is forbidden.

Publishing images of pupil and their work

- Photographs that include pupils are selected carefully so that individual pupils cannot be identified and their image misused
- Pupils' full names are not used anywhere on the website or other online space, particularly in association with photographs
- Written permission from parents or carers is obtained before photographs of pupils are electronically published
- Work can only be published with the permission of the pupil and parents/carers
- The copyright of all material is held by the school, or is attributed to the owner where permission to reproduce has been obtained
- Pupil image file names will not refer to the pupil by name
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social networking and personal publishing

- The school will control access to social networking sites. Safety guidance in the use of these sites will be taught during safety lessons; for example, never give personal details and to use nicknames.
- Pupils will be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Pupils will be taught only to invite known friends and deny access to others.
- Newsgroups will be blocked unless a specific use is approved. This will be accomplished through web filter blocks. (Subject Leader for Computing)

Children and young people commonly use electronic equipment including mobile phones, tablets and computers on a daily basis to access the internet and share content and images via social networking sites such as Facebook, Twitter, MSN, Snapchat, Instagram and TikTok which is a video-sharing social media app available on iOS and Android which lets users create, share, and view user created videos much in a similar manner to Facebook, Instagram and Snapchat. It's main draw, however, is that users can record and upload bite-sized looping videos of themselves lip-syncing and dancing to popular music or soundbites, often for comedic effect, which can then be further enhanced with filters, emojis and stickers. TikTok has been designed with the young user in mind and has a very addictive appeal.

These technologies and the internet are a source of fun, entertainment, communication and education. Unfortunately, however, some adults and young people will use those technologies to harm children. That harm might range from sending hurtful or abusive texts and emails to grooming and enticing children to engage in sexually harmful conversations, webcam photography or face-to-face meetings. Pupils may also be distressed or harmed by accessing inappropriate websites that promote unhealthy lifestyles, extremist behaviour and criminal activity.

New technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- The senior management team should note that technologies such as mobile phones with wireless internet access to (3G/4G roaming) can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The appropriate use of Learning Platforms (Fronter) will be upheld by all members of staff and all children will be provided with a personal safe and secure username and password.

Protecting personal data

Personal data will be recorded, processed, transferred and made available in accordance with the requirements of the Data Protection Act 1988.

Policy decisions

Authorising internet access

- The school allocates internet access for staff and pupils on the basis of educational need.
- Pupils accessing the internet are directly supervised by a member of the school staff at all times.
- Parents are informed that pupils will be provided with supervised internet access and are asked to return a consent form agreeing to school procedures for monitoring pupil use of the internet.
- Any person not directly employed by the school will be asked by the Head teacher to sign the 'Acceptable use of Internet' Policy before being allowed to access the internet from the school site.

See Appendices 2

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school. Neither the school nor Local Authority can accept liability for any material accessed, or any consequences of internet access. However, methods to identify, assess and minimise risks will be reviewed regularly. The Head teacher will ensure the Online Safety Policy is implemented and compliance with the policy will be monitored. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Complaints procedures

- Prompt action is required if a complaint regarding the inappropriate use of the internet is made. The facts must be established quickly, for instance whether the internet use was within or outside school.
- Complaints connected to internet misuse will be dealt with by the Head teacher or a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be referred to the school Designated Child Protection Officers (Miss Jaggers or Mrs Lord) and dealt with in accordance with child protection and safeguarding procedures.
- Pupils and parents will be informed of consequences for pupils misusing the internet. A minor transgression of the rules may be dealt with by the teacher as part of normal class disciplinary sanctions.
- Situations of a potentially serious nature, will be subject to a range of sanctions including:
  - interview by Head teacher
  - informing parents or carers
  - removal of internet or computer access for a period of time
  - possible referral to Kingston's social services
- Pupils and parents will be informed of the school's complaints procedure (see Complaints Policy)
- Parents and pupils will be required to work in partnership with the school to resolve any serious issues regarding misuse of the internet.
- As with other safeguarding issues, there may be occasions when social services or the police will be contacted.

Cyberbullying

At Malden Parochial we deal with reported incidents of virtual or cyberbullying in accordance with our Anti-bullying Policy.

We acknowledge that silent phone calls, abusive messages and comments on social networking sites can be very distressing and accept that this kind of bullying needs to be investigated and dealt with accordingly. All incidents of virtual or cyberbullying will be reported to the Head teacher and Online Safety Officer who will then take the responsibility for the investigation and management of the incident. This may include a meeting with parents or a letter outlining our concerns.

The victim will receive appropriate support and if necessary the police will be informed of the situation. Staff may seek further advice and support with regards to virtual or cyber bullying from their professional association or union.
Victims of virtual or cyber bullying are advised to:

- Save messages and texts
- Never to reply
- Block future messages
- Report the incident

Prevention of virtual and cyberbullying

All staff will be supported in their knowledge and understanding of the technologies pupils are using both inside and outside school. Regular training and updates will be provided by the Subject Leader for Computing and Online Safety Co-ordinator. The subject of bullying (in all its forms) will be regularly covered through Collective Worship, themed weeks, PSHCE lessons and circle time.

Meetings for parents/carers will be organised to give information and advice about internet safety. On an annual basis pupils, staff, parents and governors will be involved in monitoring, evaluating and improving policies and procedures.
See Appendices 4 and 5

Radicalisation/Prevent strategy

The Counter-Terrorism and Security act (July 2015) requires authorities such as schools to "have due regard to the need to prevent people being drawn into terrorism." This is known as the 'prevent duty'. The Department of Education (DFE) States that protecting pupils from risk of radicalisation should be seen as part of schools wider safeguarding duties. It says it is similar in nature to the duty to protect pupils from harm caused by, for example drugs, gangs, neglect or sexual exploration. All schools are covered by the Prevent duty.

The objectives of the Prevent strategy are to:-

- Respond to the ideological challenge of terrorism and the threat we face from those who promote it
- Prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support
- Work with sector and institutions where there are risks of radicalisation that we need to address.

The school will:-

- explore and promote diversity and shared values between and within communities;
- maintain an appropriate filtering system for the internet;
- safeguard school based emails and logins. The Subject Leader for Computing to have access and the ability to close down school email accounts if they are misused or if any outside emails pertaining to radicalisation have infiltrated the system. The Subject Leader for Computing will immediately block key phrases and words on the filters; and,
- ensure that staff are given training that enables them to identify pupils at risk of being drawn into terrorism and challenge extremist ideas.

Communications Policy

Introducing the online safety scheme of work for pupils

- E-safety lessons will be taught each term as part of the curriculum following an agreed scheme of work which develops skills that children need to achieve across the key stages.
- Pupils will be informed that network and internet usage will be monitored and will be followed up if necessary.

- Instruction and reminders about responsible and safe use of the internet will precede every lesson which includes internet access.
    - ➢ Online safety posters will be displayed in the Computing Suite and next to computers within the classroom so that all users can see them.
    - ➢ Each year the children will create their own up to date version of an internet code of conduct. *See Appendix 1*

Staff and the E-safety Policy

- The Online Safety Policy will be available to all stakeholders via the school website.
- Staff should be aware that network and internet traffic can be monitored and traced; discretion and professional conduct is essential.
- The monitoring of internet use is a sensitive matter. Staff that manage filtering systems or monitor IT use will be supervised by senior management.
- Staff will use a child friendly safe search engine when accessing the web with pupils and common search terms will have been checked prior to the lesson

Ensuring parent/carer support

- Parent’s attention will be drawn to the school’s Online Safety Policy in newsletters, workshops and conversations.
- Parents will be notified on regular base of new ways of keeping their children safe online and regular school involvement in activities such as the national Online Safety Day (usually held in February) will promote keeping children safe online.
- School website will include a list of up to date e-safety resources.
- Internet issues will be handled sensitively, and parents/carers will be advised accordingly.
- A partnership approach with parents will be encouraged.
- The school will ask new parents to sign the parent/pupil agreement – with respect to internet usage.

Internet use in pupils’ homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the internet. The school should help parents plan appropriate, supervised use of the internet at home if requested.

If parents wish to share images e.g. photographs of their child for inclusion in newsletters etc. these must be sent via an encrypted email.
See appendix 3 and 6

Concluding statement

At Malden Parochial we believe that all pupils and staff should have access to the internet regardless of race, culture, age, ability or gender. We endeavour to ensure that all access is monitored and that only appropriate resources are used on our school site.