MARYLAND PRIMARY SCHOOL

Online Safety POLICY

Updated November 2023

Aim

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Safeguard effectively from all 4 categories of risk in relation to: content, contact, conduct, commerce.
    - ★ Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
    - ★ Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
    - ★ Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
    - ★ Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Ensure our processes and approaches to online safety are regularly reviewed against the latest technologies and risks (using tools such as https://360safe.org.uk/)

The Online Safety Policy should be read in conjunction with the Safeguarding, Behaviour and Anti-Bullying policies.

Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

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

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

Roles and responsibilities

Headteacher

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

Senior Leadership Team

- To take overall responsibility for online safety provision
- To take overall responsibility for data and data security
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- To be responsible for ensuring that staff receive and complete training
- To be aware of procedures following a serious online safety incident
- To ensure that staff, private providers /visitors and volunteers in the school adhere to the school's online safety policy.

Designated Safeguarding Lead

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

Online Safety Lead

- Work with the leadership team and school based technician, to ensure that appropriate filtering and monitoring is in place.
- Take appropriate action in line with child protection policies and procedures, if the filtering system and monitoring approaches identify any causes for concern.
- Working with the headteacher, computing lead and other staff, as necessary, to address any online safety issues or incidents
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- Ensuring that any online safety incidents including cyberbullying are logged and dealt with appropriately
- Updating and delivering staff training on online safety

Computing Lead

- To take responsibility for the online safety curriculum and schemes of work and monitor the delivery of this
- Liaise with the school technician regarding hardware and software matters

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Teachers

- Teach online safety lessons, following the timetable and schemes of work provided by the Computing Lead
- To complete training provided by the Online Safety Lead or Computing lead
- 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, and ensuring that pupils follow the school's terms on acceptable use
- Working with the online safety lead to ensure that any online safety incidents are logged and dealt with appropriately
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes.
- Following the correct procedures by contacting computing lead if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

School based technician

- To report any online safety related issues that arise to the Computing Lead and Senior Leaders
- To ensure that access controls/encryption exists to protect sensitive information

Governors

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.
- To approve the Online Safety Policy and review the effectiveness of the policy

Parents

- Every week we send out an online safety reminder to parents and staff. It is the parents duty to discuss the message with their children.
- Regarding Primary children creating social media accounts, such as Youtube and Facebook, the NSPCC advice is that the school cannot prevent a child from creating accounts, it is the responsibility of the parents.
- Youtube, Discord, Tiktok, Instagram and Snapchat all require a minimum age of 13.
- Online chat services again it is the parents' responsibility to monitor their child's online activity and age requirement. For example, Whatsapp requires a minimum age of 16.
- All parents are sent online safety posters by the school to advise parents how to check their child's device to ensure the appropriate settings are in place.

- Parents can contact the school's E-safety team for advice.
- Online safety takes high priority in our school.
- Online safety is now taught throughout the year
- There has been a whole cm review to ensure online is covered by all year groups in KS1 and 2.
- The new Cm map is published on our website – it is taught from Autumn to Summer – and the policy is on the website on the Key Policies tab.
- It is also taught through CPSHE where mental health and getting 'likes' is discussed and children are provided with strategies on how to overcome online issues.
- We also get links from NSPCC who provide staff with tips on how to deal with online issues. It is also part of DSL training.
- All teachers have had their yearly online safety training.
- Both KS1 and 2 have regular online safety assemblies throughout the year touching on the most relevant issues at the time.
- We have an E-Safety board which is updated regularly, including a worry post box where children can anonymously post their concerns.
- Our online safety lead is our assistant head teacher but we work as a team which includes the DSLs, Senior Behaviour Mentor and our Computing lead teacher.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Training

All staff members will be trained on online safety annually, as part of their safeguarding training, this includes abuse where digital devices can be used such as sexting, upskirting, bullying, sexual violence and harrassment, etc. It is the responsibility of the Designated Online Safety & Computing Lead to keep up to date with changes to technology and online safety risks and inform staff of any changes Training will also take place throughout the year via staff updates, bulletins, case studies, etc.

Working in partnership with parents

We understand the importance of working closely with parents and aim to keep parents informed about online safety. All parents sign their agreement to the school's online safety rules in the home-school agreement. We also keep parents and carers informed of online safety issues via:

- The school website (including the CEOP button where they can report certain concerns directly to the police)
- Newsletter updates and reminders via ParentMail
- Online safety workshops
- Meetings with the Senior Leadership Team / Online DSL

Educating pupils about online safety

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

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- *That people sometimes behave differently online, including by pretending to be someone they are not*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

Managing online safety risks within school

The internet is an essential element of education and the school has a duty to provide pupils with quality internet access as part of their learning experience. The school ensures that appropriate filtering systems are used. The school's internet access is regulated by LGFL (London Grid For Learning). This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools. Students have a set of blocked categories which they are unable to access using the school's network, which differs from staff's blocked categories.
The internet access we provide is a 'managed' system rather than a 'locked down' system, in accordance with Ofsted 2014 guidance that these allow pupils with the opportunities to learn how to assess and manage risk for themselves. Governors and Senior Leaders conduct internet filter checks termly.

Pupils are given Google Suite for Education accounts which are used to log into the school's computer network. Alerts are sent to admin accounts (ie. designated online safeguarding lead) to inform them of any suspicious activity eg. unusual log-in attempt.

Online safety agreements

All pupils agree to a set of online safety rules at the beginning of the academic year and sign to show their agreement. If pupils break any of these rules, they may receive sanctions in line with the school's behaviour policy. In situations where pupils repeatedly break the online safety rules or there is a serious breach, they may be temporarily banned from using the school's technology. Year 6 & Year 5 pupils who bring mobile phones into school also adhere to the schools Mobile Phone Protocol.

All members of staff sign an online safety agreement and a code of conduct.

Dealing with online safety incidents

Concerns about online safety should be referred to the Designated Online Safeguarding Leader or Computing Lead in the first instance. These members of staff will investigate the incident, including interviewing pupils and staff where necessary. Parents and carers will be informed about online safety incidents involving their children and advised about how to prevent further incidents. Where incidents involve a possible breach of the law, the police will be informed.

The school may investigate online safety issues that take place outside of school, in line with our safeguarding requirements and our commitment to anti-bullying and pupil wellbeing.

Any concerns regarding a member of staff's use of the internet should be referred to the Headteacher, in accordance with whistleblowing procedures.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from a computing lead or school based technician.

Online Remote Learning Guidelines

Guidance for parents & pupils has been published on the school website for ease of reference - this includes:

- Safeguarding advice eg. parental controls
- Process to report online concerns

Guidance for staff is shared during training opportunities and can be accessed via the school's Google system.

Pupils can access their acceptable user agreements online for reference and have secure usernames and passwords to access their work via Google Classroom.

Social Media

Maryland Primary School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online. Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (for staff & governors).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the designated online safeguarding lead will request that the post be deleted and will expect this to be actioned promptly.

We will also aim to prepare Children for using social media. For example we will help them to understand what *cookies are (given their permission is requested on every website), how we are the product for sale on social media sites and how they gather information for advertisers, how misinformation can spread, how doctored images can affect a child's perception of their own body image etc.*

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Maryland recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Maryland will treat any use of AI to bully pupils in line with our behaviour policy.

Pupils using mobile devices in school

Please refer to Maryland's Mobile Phone Protocol