Mayflower Primary School

Online Safety Policy

Approved by: Governing Body	Date: March 2024
Next Review Date by: March 2025	

This policy is a living document, subject to statutory annual review and amended, when necessary, throughout the year in direct response to developments that may occur internally within school, the local area and/or government advice. This policy document has been produced to ensure the protection of all parties - pupils, staff, governors and the wider community.

The purpose of this policy statement is to:

• Provide clear advice and guidance on how to minimise risk.

• Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices.

• Provide staff and volunteers with the overarching principles that guide our approach to online safety.

• Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

Related policies and procedures:

This policy statement should be read alongside our organisational policies and procedures, including:
• Child protection

• Procedures for responding to concerns about a child or young person's wellbeing

• Dealing with allegations of abuse made against a child or young person

• Managing allegations against staff and volunteers

• Code of conduct for staff and volunteers

• Anti-bullying policy and procedures

• Photography and image sharing guidance

'Keeping Children Safe in Education 2023' groups online safety risks into four areas known as the 4 C's. They do not stand in isolation, however, and it is important to understand the interplay between them.

Content	Being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
Contact	Being subjected to harmful online interaction with other users; for example: 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	Online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images.
Commerce	Risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Rationale

Mayflower Primary School uses the internet in a variety of ways including :

• To aid delivering a high achieving, broad and balanced curriculum,

• To promote pupil achievement and manage/sustain online learning,

• To support the professional work of all staff

• To enhance the school's management information and administration systems

We recognise that:

• The online world provides everyone with many opportunities; however, it can also present risks and challenges.

• We have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online.

• We have a responsibility to help keep children and young people safe online, whether or not they are using Mayflower School's network and devices.

• Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

• All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

We will seek to keep children and young people safe by:

- Appointing an online safety coordinator (computing lead) to work closely with the designated safeguarding lead.
- Providing clear and specific directions to staff and volunteers on how to behave online through our acceptable use policy and behavioural code for adults.
- Supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- Supporting and encouraging parents and carers to do what they can to keep their children safe online.
- Developing an online safety (acceptable use) agreement for use with young people and their parents or carers.
- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person.
- Reviewing and updating the security of our filtering and monitoring information systems regularly.
- Ensuring that usernames, logins, email accounts and passwords are used effectively and kept secure.
- Ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate.

- Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given.
- Providing supervision, support and training for staff and volunteers about online safety.
- Examining and risk assessing any social media platforms and new technologies before they are used within the organisation.
- Ensuring compliance with all relevant legislation connected to this policy.

The use of such technology greatly enhances communication and the sharing of information. At Mayflower Primary School, pupils and staff are to be encouraged to use them in a safe, positive and responsible way. However, their use can put young people at risk within and outside of school.

Some of these dangers include:

• Access to illegal, harmful or inappropriate images or other content

• Unauthorised access to / loss of / sharing of personal information

• The risk of being subject to grooming by those with whom they make contact on the Internet

• The sharing / distribution of personal images without an individual's consent or knowledge

• Inappropriate communication / contact with others, including strangers

• Cyber-bullying

• Access to unsuitable video / Internet games

• An inability to evaluate the quality, accuracy and relevance of information on the Internet

• Plagiarism and copyright infringement

• Illegal downloading of music or video files

• The potential for excessive use which may impact on the social and emotional development and learning of the young person

Mayflower Primary School is very aware of the vulnerability of our SEND pupils with regards to online safety. As such, a specific SEND acceptable use agreement is used for pupils who may require it. The home school-partnership with these families is especially vital to ensure that the risks posed for these pupils are minimised as much as possible. Risk management and at home strategies should also be discussed in annual reviews for those pupils concerned.

Roles and Responsibilities:

Mayflower Primary School adopts a whole school approach when promoting online safety. This policy applies to all pupils, parents and carers, teaching and support staff, governors, students, part-time staff, mid-day supervisors, music tutors, sports coaches, volunteers and visitors. This list is not to be considered exhaustive.

The role of the Designated Person/s for Child Protection:

- To attend training on online safety issues and be aware of the potential for serious child protection issues which arise from:
    - ✓ Sharing of personal data
    - ✓ Access to illegal / inappropriate materials
    - ✓ Inappropriate on-line contact with adults / strangers
    - ✓ Potential of actual incidents of grooming
    - ✓ Cyber-bullying

- To provide support and advice to staff as regards potential online-safety issues.
- To liaise with the Computing subject leader and other staff in regard to the implementation and monitoring of the online safety programme of work.
- To update the Head Teacher and Governors of any online safety issues that need attention.

The Role of Teaching and Support Staff:

- To have an up-to-date awareness of online safety matters and of the current school policy and practices related to online safety.
- To report any suspected misuse or problem to the designated person/s for child protection for investigation / action / sanction.
- To ensure any digital communications with pupils are on a professional level and only carried out using the official school systems.
- To ensure personal information, including telephone contact details and personal social media accounts, are not provided to pupils.
- To carry out the school's digital literacy/online learning programme of work and embed it in everyday practice in all aspects of the curriculum.
- To ensure pupils understand and follow the online-safety rules. A copy should be easily accessible to the pupils; for example, displayed in the classroom/communal school building or made digitally accessible via the year group computing sites. The copies available should be appropriate for the age and understanding of pupils (EYFS, KS1, KS2) and parents and carers.
- To ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- To monitor computing activity in lessons and extra-curricular / extended school activities as appropriate.
- To be aware of online-safety issues related to the use of mobile phones, cameras and handheld devices which should not be within the children's possession in school unless given permission.
- To ensure that in lessons where use of the internet is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with unsuitable material that is found in Internet searches.
- To understand the contents of this policy and other e-safety related policies and to sign the Staff Acceptable Use Policy (see Appendix 1).
- To ensure they are familiar with the latest KCSIE 2023, particularly paragraphs 135-147 pertaining to the implementation of online safety strategies in education.
- To attend/complete online safety training assigned digitally or in person.

The Role of Pupils:

- To abide by the school's rules for safe Internet use.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- To abide by the school's policy as regards to the use of mobile phones, cameras, Laptops, iPad's and chrome books.
- To understand the importance of adopting secure, well -informed online-safety practices outside of school.
- To understand and abide by the school's anti-bullying, mobile phone and acceptable use policies.
- To avoid plagiarism and uphold copyright regulations.

The Role of Parents and Carers:

Parents and carers play a crucial role in ensuring that their children understand the need to use internet and their mobile devices in an appropriate way. All parents must sign their child's acceptable use policy which further explains parental guidance pertaining to the use of digital devices and navigating them safely both in school and at home. The school will take every opportunity to help parents understand these issues through welcome meetings, parents' evenings, newsletters and ensuring the regular upkeep of our school website. All parents are actively encouraged to attend parent online safety workshops and should take the time to understand the contents of this policy.

Curriculum:

The school uses a broad and balanced curriculum that focuses on the three pillars of progression within Computing – digital literacy, computer science and information technology. The use of the internet is necessary within all three strands. Digital literacy (online safety) is the first unit taught in each year group throughout Mayflower Primary School and is regularly revisited through short stand-alone sessions and cross-curricular links with subjects such as RSE & PSHE. In Computing lessons and school assemblies – lead by our Computing lead and digital leaders – there is dedicated teaching about how to deal with issues that may arise in the digital world. Online Safety is embedded across the curriculum as we regularly encourage pupils to use iPads to enhance their learning.

Use of digital and video images:

Examples of how digital photography and video may be used within the school include:

- Pupils being photographed by the class teacher, teaching assistant or other pupils as part of a learning activity e.g. photographing pupils at work which may be displayed or recorded on our online learning journey or school X account. These images will be taken using the allocated classroom iPad devices.
- A pupil's image for presentation purposes around the school e.g. on school displays promoting pupil leadership.

- A pupil's image being used for promotional literature such as the school prospectus, website, year group Google Page, Instagram, or Twitter account.
- On rare occasions, a pupil's image may appear in the media if a newspaper photographer or television film crew attend a school event.

NOTE: If a circumstance arose where the school wanted to link a pupil's image to their name e.g. if the pupil won a national competition and wanted to be named as a result of this, parental permission would be sought separately on these occasions.

The following safeguarding principles are followed with specific regard to the use of digital and video images:

• The school will gain parental/carer permission for the use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school and recorded on our internal administrative system (RM Integris) ensuring all class teachers are aware of permissions of individual children.

• Only images of pupils in suitable dress are used.

• Parents volunteering on class trips are not allowed to take photographs or videos on their personal equipment.

• Any digital videos or images of pupils should only be saved on the school Teams SharePoint point drives or on the school Google Drive.

• The school does not identify pupils in online photographic materials or include the names of pupils in any materials published by the school.

• All staff sign the school's 'Acceptable Use Policy' and this includes a clause on the use of mobile phones and personal equipment for taking pictures of pupils.

• The school blocks/filters access to social networking sites/blogs unless there is a specific approved educational purpose.

• Pupils are advised to be very careful about placing any personal photos on any social online network space. They are taught to understand the need to maintain privacy settings so as to not make public any personal information.

• Pupils are taught that they should not take or post images or videos of others without their permission. They are taught about the risks associated with providing information that reveals the identity of others and their location such as address or school name. Pupils are taught about the need to keep their data secure and what to do if they are subject to bullying and abuse online or offline.

• Explicit permission must be gained from parents to use their child's images on school material, the website, or X (Formerly known as Twitter). All members of staff are encouraged to familiarise themselves with permissions via RM Integris.

Website:

The Senior Leadership Team alongside the admin Team take overall editorial responsibility to ensure that the website content is accurate and well presented.

• Uploading of information is restricted to approved website editors.

• The school website complies with the school guidelines for publications.

• Most material on the website will be the school's own work; where others work is published or linked to, the school will credit the sources used and clearly identify the author.

• The point of contact on the website is the school address, telephone number and office email address: admin@mayflower.towerhamlets.sch.uk

• Photographs published on the website will not include any names.

• Pupil names will not be used when saving images or in the tags when publishing to the school website.

X (Formerly known as Twitter)

The school has its own X account which are used to communicate information and pictures which are of interest to parents, the local community and a wider audience of followers.

The following safeguarding principles have been put in place:

• Permission to 'upload' to X or Instagram is authorised by the Headteacher. At present, all teaching staff can upload to X. Before posting, teachers must check content with another member of staff to ensure posting guidelines are being followed.

The content of all photos and videos that are uploaded will follow the same guidelines as set out in this document.

• The designated members of staff responsible for the X account will regularly check any comments that are posted and check the suitability of those 'following' the school's account. They will take the necessary steps to delete/block any comments or followers deemed inappropriate.

E-mail & Microsoft Office 365:

• All staff and students have access to Microsoft Office 365

• Microsoft Teams will be regularly monitored by class teachers and the computing coordinator to ensure safe and sensible use by all students.

• Online chat features (Teams stream, Teams meet) should only be made accessible to students when used in real time with class teachers.

• Pupils will be encouraged to tell a member of staff if they receive any offensive communication via our online platforms.

• Pupils will be taught to not reveal personal information about themselves or others in e-mail communication or arrange to meet anyone with parental permission and agreement.

• Access to personal, external e-mail accounts may not always be possible if certain e-mail sites are blocked by our filter and monitoring.

• School e-mail messages sent to organisations should be written carefully and checked before sending, in the same way that a letter written on school headed paper would be.

• Staff should use the school e-mail system for official school business only. All staff should be made aware that e-mail messages are subject to 'freedom of information' requests in the same way as other information is within the school setting.

Filtering & Monitoring

The filtering of Internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is important that the school's filtering policy is regularly monitored and updated and able to manage the associated risks. The school will continue to subscribe to the filtering service provided by the London Grid for Learning (LGfL) and their appointed service provider (currently Virgin Broadband). The school will apply the suggested website filters; but will maintain the ability to block / un-block certain sites when any reasonable request is made, and the relevant website is checked for suitability. Test - filtering.com is carried out by CleverICT monthly.

The members of staff able to make changes to the school's filtering policies are:

• The Headteacher

• The Computing Lead

• The School Business Manager

• Appointed ICT technicians

Communication of Policies:

Pupils

• Pupils will be made aware that Internet use will be monitored

• All pupils who access the Internet will be asked to sign an age appropriate 'Acceptable Use Policy'.

Staff

• All staff will be given a copy of the school's online-safety policy and will have an opportunity to discuss its content.

• All staff will be made aware that the use of the Internet in school should be for educational purposes only and that Internet traffic can be monitored and traced back to the individual user. Discretion and professional conduct is essential.

• All staff will be asked to sign an 'Acceptable Use Policy'

• All staff will be required to attend any online-safety training deemed necessary by the school leadership team or online-safety co-ordinator.

Parents / Carers

• Parents' attention will be drawn to the school's online-safety policy through the appropriate means (email, website, CC Computing site).

• Parents must sign and discuss the 'Acceptable Use Policy' with their child(ren).

• Parents will be encouraged to discuss with the school any concerns / questions they have with regard to the safety of their child(ren) whilst on-line.

• Parents will be invited to regular online safety meetings to discuss any concerns they may have, as well as to educate themselves about how to keep their young people safe online.

• Parents will have access to government approved online safety resources via the main school website and computing site.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class Teachers will discuss cyber-bullying with their classes and the issue will be addressed in assemblies. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. The school also provides information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

Conclusion:

As with all other risks, it is impossible to eliminate them completely. It is therefore essential, through high standard educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with them as and when they present themselves.

If online abuse occurs, we will respond to it by:

• Having clear and robust safeguarding procedures in place for responding to online abuse.

• Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation.

• Making sure our response takes the needs of the person experiencing abuse, any bystanders and our school as a whole into account.

• Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

This online safety policy will enable the school to demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably expected of them to manage and reduce these risks.

Supporting documents:

DfE, Keeping Children Safe in Education, 2023
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

• DfE, Meeting digital and technology standards in schools and colleges, 2023 Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

• DfE, Relationships Education, Relationships and Sex Education (RSE) and Health Education, 2021 Relationships and sex education (RSE) and health education - GOV.UK (www.gov.uk)

• DfE, Safeguarding and remote education, 2022 Safeguarding and remote education - GOV.UK (www.gov.uk)

Contact details:

Online safety co-ordinator Name: Kalshuma Begum

Designated Safeguarding Lead Name: Dee Bleach

Phone/email: dee@mayflower.towerhamlets.sch.uk

We are committed to reviewing our policy and good practice annually.