Muswell Hill Primary School

E-Safety Policy

Agreed: July 2017

Review: September 2020 in line with Remote Learning Policy, Appendix to Remote Learning Policy and Safeguarding Online Child Protection Policy/August September 2020 & Muswell Hill Primary School Blended Learning Policy and Practice

The E-Safety Policy will be reviewed in Spring 2021

Muswell Hill Primary School is a Rights Respecting School, based upon the UNICEF Convention of the Rights of the Child.

We believe that all children should grow up aware of these rights and respect these rights for themselves and for others. Being a Rights Respecting School underpins policies throughout the school. As policies are reviewed within the cycle they are adapted to demonstrate this. **Reviews started in the academic year of 2019/20. The school received the Bronze Award in July 2020 and is currently working towards the Silver Award.**

School Vision & Values

At Muswell Hill Primary we have worked hard to create a successful, high achieving, happy, inclusive community. One we are proud of and one which enables us to work in partnership with others, celebrate our successes and empower our children to be the best versions of themselves. Our community is where friendships thrive and where children are encouraged to discover a world of possibilities in a challenging yet supportive setting. Here at Muswell Hill Primary School, we embrace the joy of learning every day, through our strong, rich, broad curriculum.

Muswell Hill really is an extraordinary school**. Muswell Hill is underpinned by the values:**

Creativity Integrity Resilience Respect Curiosity

To all our pupils, this is our commitment:

At Muswell Hill Primary School, the staff and governors are working every day so that by the time you leave us:

- You will love learning new things, feel ready for the future and want to keep on learning.
- You will understand how you learn best, learn from your mistakes and how to persevere.
- You will know what it feels like to be motivated to be good at something, and to have achieved your very best.
- You will understand just how incredible you are! You will believe in yourself and have the confidence to follow your dreams.
- You will have grown as healthy and strong as you can, and you will know how to look after your body and your mind.
- You will know friendship and will have learned how to get along with other people.
- You and your family will be supported and cared for if you struggle or meet obstacles during your time with us.
- You will feel part of your community, proud of your school, and inspired to make a difference.
- You will leave Muswell Hill with lots of good memories and be the best version of yourself.

Aims/Mission: ***Everyone belongs here, everyone has a voice and everyone is heard***

Policy Statement

ICT and the Internet have become integral to teaching and learning within schools, providing pupils and staff with opportunities to improve understanding. However, whilst this technology has many benefits for Muswell Hill Primary School (MHPS), we recognise that clear procedures for appropriate use and the education of staff and pupils about online behaviour and potential risks are essential.

This Policy covers all technology-based platforms and devices (including personal) used by staff, pupils, visitors and contractors within the school grounds and school-issued devices for use off-site.

Aims of this policy

- EDUCATE: To emphasise the need to educate staff, pupils and parents about the safe use of technologies both within and outside the school environment.
- SAFEGUARDS AND RULES: To provide safeguards and rules for acceptable use to guide all users in their online experiences.
- PROCEDURES IN THE EVENT OF MISUSE: To ensure teachers and pupils are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.

Educate

Teaching and Support Staff

The school strives to ensure that all teaching and support staff (including volunteers) read and understand the Acceptable Use Policy for School-based Employees (Appendix 1). A copy of this document is retained in the Headteacher’s office and is made available to all staff, and appropriate volunteers, visitors and contractors.

Pupils

The school strives to embed E-Safety in all areas of our curriculum, and key online safeguarding messages are reinforced wherever ICT is used in learning. The Acceptable Use Policy for Pupils is provided to every pupil in writing, Appendix 2.

Pupils must:

- abide by the Acceptable Use Rules for Pupils
- use the Internet and technologies in a safe and responsible manner within school
- inform staff of any inappropriate materials, cyber-bullying or contact from unknown sources

All pupils and their parents/carers will receive a copy of the Acceptable Use Rules on first time entry to MHPS. Pupils and their parents/carers are asked to read and abide by the rules.

Safeguards & Rules

The following areas will be addressed and monitored to ensure that MHPS is providing a safe environment for pupils and staff:

- Anti-virus software and appropriate filtering of Internet content
- All school ICT equipment (including serial numbers) to be logged when issued to staff
- No personal or sensitive data to be stored on school or personal devices
- No personal devices to be used within the classroom or for school-related activities other than provision of emergency contact details for off-site activities

Written consent will be obtained from parents or carers before photographs or videos of young people are used within the school environment, including the school website or associated marketing material. Pupils' identities will not be exposed and any narrative will be generic.

Procedures in the Event of Misuse

In the event of misuse by staff or pupils, including use of the school network in an illegal, unsuitable or abusive manner, a report must be made to the Headteacher or Local Authority Designated Officer (LADO) for Safeguarding immediately.

In the event of accidental misuse, a report must be filed with the Headteacher and recorded in the E-Safety log (Appendix 3).

In the event of intentional misuse, internal investigations will be initiated and disciplinary procedures followed. Additionally, all security breaches, lost/stolen equipment or data, unauthorised use or suspected misuse of ICT should be reported immediately to the Headteacher.

All incidents will be recorded on the E-Safety Incident Log to allow for monitoring, auditing and identification of specific concerns or trends.

Appendix1: Acceptable Use Policy for School-based Employees

Policy Statement

In order to create a safe teaching and learning environment, effective policies and procedures which are clearly understood and followed by the whole school community are essential. This Acceptable Use Policy sets out the rules, responsibilities and procedures for the safe and appropriate use of all technologies; its aim is to safeguard adults, children and young people within a school or educational setting. The Policy recognises the ever-changing nature of emerging technologies, and highlights the need for regular review to incorporate developments within ICT.

The purpose of the Acceptable Use Policy is to clearly identify for the whole school community:

- the steps taken in school to ensure the E-Safety of pupils when using the Internet, e-mail and related technologies
- the school's expectations for the behaviour of the whole school community whilst using the Internet, e-mail and related technologies within and beyond school
- the school's expectations for the behaviour of staff when accessing and using data

Scope of the policy

The policy applies to all school-based employees and volunteers.

Responsibilities of the Headteacher and Governors

The Headteacher and Governors have overall responsibility for E-Safety as part of the wider remit of safeguarding and child protection, and must appoint an E-Safety Lead to implement agreed policies.

All employees, pupils and volunteers should be aware of who holds this post within MHPS. The school will:

- provide a safe, secure and appropriately filtered Internet connection for staff and pupils within the school
- promote E-Safety across the curriculum
- ensure that no equipment that holds sensitive or confidential information leaves school premises
- share any E-Safety progress and curriculum updates at all governing body meetings and ensure that all present understand the link to child protection.

- ensure that E-Safety is embedded within all child protection training, guidance and practices

E-Safety Lead

The nominated E-Safety Lead will:

- recognise the importance of E-Safety and understand the school's duty of care for the E- Safety of its pupils and employees
- ensure that all individuals in a position of trust who access technology with pupils understand how filtering levels operate and their purpose

Individual Responsibilities

All school-based employees and volunteers must:

- take responsibility for their own use of technologies and the Internet, making sure that they are used legally, safely and responsibly
- ensure that pupils in their care are protected and supported in their use of technologies so that these can be used in a safe and responsible manner. Children must be informed about what to do in the event of an E-Safety incident
- report any E-Safety incident or concern or misuse of technology to the E- Safety Lead or Headteacher
- use school ICT systems and resources for all school-related business and communications
- ensure that all electronic communication with pupils, parents, carers, employees and others is compatible with their professional role
- ensure that personal details, such as mobile numbers, social network details and personal e- mail must not be shared or used to communicate with pupils and their families
- not post online any text, image, sound or video that is incompatible with their professional role
- protect their passwords/personal logins and log-off the network wherever possible when leaving work stations unattended
- understand that if they ignore security advice or use e-mail or the Internet for inappropriate reasons they risk dismissal and possible police involvement, if appropriate

Staff should know the legal age that children are allowed to use particular social media platforms such as Facebook, Instagram and Twitter.

Appendix 2: Acceptable Use Rules for Pupils

Teaching staff should cover these principles with the pupils as an on-going concern, but the principles should be highlighted formally on an annual basis in an effort to educate pupils about online safety.

Key Stage1 Online Rules

- We learn how to use the Internet safely.
- We can send and open messages with an adult.
- We can write polite and friendly e-mails or messages to people that we know.
- We only tell people our first name.
- We learn to keep our password a secret.
- We know who to ask for help.
- If we see something we do not like, we know what to do.
- We know that it is important to follow the rules.
- We are able to look after each other by using the Internet safely.
- We can go to www.thinkuknow.co.uk for help.

Pupils should know the legal age that they are allowed to use particular social media platforms such as Facebook, Instagram and Twitter

Key Stage 2 Online Rules

- We use the Internet to help us learn, and we know how to use it safely and responsibly.
- We send e-mails and messages that are polite and friendly.
- We will only e-mail, chat or go on webcam with people that we know in real life, with permission from our teachers or parents.
- We make sure that an adult always knows when we are online.
- We never give out passwords or personal information (like our full name, school or address).
- We never post photographs without permission, and never include names with photographs.
- We know who to ask if we need help.
- If we see anything on the Internet or on e-mail that is scary or makes us feel uncomfortable, we know what to do.
- We never open e-mails or links from people we don't know.
- We know that the rules are there to keep us safe and must not be broken.
- We are able to keep ourselves and each other safe by using the Internet in a responsible way.
- We can go to www.thinuknow.co.uk for help

Pupils should know the legal age that they are allowed to use particular social media platforms such as Facebook, Instagram and Twitter

Appendix 3:

EXAMPLE E-Safety Log – to be maintained by Headteacher

Muswell Hill Primary School E-Safety Incident Log

Date of incident	Name of individual(s) involved	Device number/ location	Details of incident	Actions and reasons	Confirmed by
20/01/2016	Joe Smith	PC 1 Blue Class	Child accessed inappropriate chat site using child log- in. Adult language used	Hector Protector launched effectively by young person. Website now blocked and filtering levels	David Howes

CYBER-BULLYING POLICY

Definition

Cyber-bullying occurs when someone is tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted by another child, pre-teen or teen using the Internet, interactive and digital technologies or mobile phones. There has to be a minor on both sides.

MHPS is committed to developing a safe environment where the pupils act respectfully and positively towards each other in acceptable and non- threatening ways.

Procedures

Staff at MHPS have the responsibility to ensure that:

- all forms of cyber-bullying are prohibited
- they are aware of cyber-bullying and are able to look for and identify signs of occurrence among the pupils
- pupils are aware of the consequences of cyber-bullying
- all cases of cyber-bullying are reported to a member of school staff and responded to promptly
- there is supervision of technology that is effective for monitoring and deterring cyber- bullying

Pupils at MHPS have a responsibility to ensure that they:

- do not participate in cyber-bullying
- do not use mobile phones, cameras or other digital devices to record audio and visual material that is not authorised as part of the curriculum
- do not breach the privacy of pupils, staff and members of the school community through any unauthorised recording or filming
- do not disseminate inappropriate information through digital media or other means
- report incidents of cyber-bullying to a member of staff
- advise other pupils being victimised by cyber-bullying to talk to an adult
- offer to speak to an adult on behalf of the pupil who is being victimised by cyber-bullying

PREVENT

Terrorist organisations, such as ISIL, are trying to radicalise and recruit young people through an extensive use of social media and the Internet. Young people, some as young as 14, have tried to leave the UK to travel to join ISIL and other terrorist groups in Syria and Iraq.

Muswell Hill primary school recognises that,every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

We believe that we have a vital role to play in protecting pupils from the risks of extremism and radicalisation. We also believe that keeping children safe from risks posed by terrorist exploitation of social media should be approached in the same way as safeguarding children from any other online abuse.

• Our teachers are vigilant about signs of possible physical or emotional abuse in any of their pupils, if staff have a concern for the safety of a specific young person at risk of radicalisation, they should follow our **school's safeguarding procedures**, including discussing with school's designated safeguarding lead, and where deemed necessary, with children's social care.

Further details are available under school **E-Safety policy .**

Staff can also contact local police force or dial 101 (the non-emergency number). They can talk in confidence about their concerns in order to help them gain access to support and advice.

If any parents are concerned that a child's life is in immediate danger, or that they may be imminently planning to travel to Syria or Iraq dial 999 or call the confidential Anti- Terrorist Hotline.

For further details and guidance on how social media is used by terrorist organisations, such as ISIL to radicalise and recruit young people through social media please see Appendix A.

Appendix A

SOCIAL MEDIA PLATFORMS

Social media has become an essential and exciting part of how we live. Millions of young people use these platforms daily to share content. But there are a small minority of users who exploit social media to radicalise and recruit vulnerable people.

The government and police work closely with the communications industry to remove extremist and terrorist content from the Internet. Since February 2010, over 95,000 pieces of terrorist content have been removed from the Internet and the companies' below continue to work with us to limit the abuse of their platforms by terrorists and their supporters. However, more content is uploaded all the time by people from this country and elsewhere who have joined ISIL in Syria and Iraq. Many of these people have an established online identity using platforms described below.

Many community-based organisations respond to ISIL propaganda and debunk its messages. For example, London-based group Families Against Stress and Trauma (FAST) have designed an online guide for parents on the dangers of radicalisation, as well as producing a YouTube film with testimonies from parents whose children have travelled to Syria. They are currently sharing their knowledge in a series of parenting workshops.

FACEBOOK

ISIL supporters use Facebook to share content, such as news stories and YouTube videos, among their peer groups.

TWITTER

Twitter is another popular social media platform for pro-ISIL accounts and those sharing ISIL propaganda. It is easy to establish an account, stay relatively anonymous and share material with large numbers of people.

YouTube

YouTube is also used to host videos, both of official ISIL output and videos created by users themselves. Multiple ‘dummy’ accounts will be set up so that when videos are taken down they can be reposted quickly.

Users will post YouTube links across their own social media platforms in order to disseminate material, particularly Twitter and Facebook.

Ask-FM

People considering travel to Syria or Iraq sometimes use Ask.fm to ask British jihadis and female ISIL supporters about travel, living standards, recruitment, fighting and broader ideology.

The answers given by ISIL supporters are encouraging, saying all their difficulties will be solved if they travel to the region.

Instagram

Instagram is used by fighters and ISIL supporters to share the photosets frequently produced by various ISIL media organisations.

ISIL supporters also use Instagram to share pictures of their life in Syria, often showing landscapes and images suggesting they are living a full and happy life.

Tumblr

Tumblr, the blogging site, is exploited by fighters to promote longer, theological arguments for travel.

Tumblr is popular with female ISIL supporters, who have written blogs addressing the concerns girls have about travelling to the region, such as leaving their families behind and living standards in Syria.

Private Messaging

On social media, ISIL supporters frequently encourage others to message them on closed peer- to-peer networks when asked for sensitive information, such as on how to travel to the region, what to pack and who to contact when they arrive.

Popular private messaging apps include WhatsApp, Kik, SureSpot and Viber