



Mill Hill Primary School **Internet and Online Safety Policy**

Contents:

- Introduction
- Roles and Responsibilities
- Managing Pupils' Access to Technology
- Teaching and Learning
- Communications Policy
- Further Information and Links
- Appendices

Co-ordinator responsible for the policy in consultation with the staff and governors:

Computing Lead

Reviewed: January 2025

Next Review Date: January 2028

Introduction

The rapid development of technology is having an increased impact to our everyday lives. At Mill Hill, we enjoy extending our pupils' learning experiences by using technology at a variety of opportunities. However, clear guidelines need to be established and adhered to, ensuring pupils, staff and parents are aware of the potential dangers of using technology, in particular electronic communication. Safe and courteous use of the internet, texting, email, and social media sites are areas that require specific education. This is known as online safety.

Online safety highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. At Mill Hill, we understand the responsibility to educate our pupils on online-safety issues, teaching them the appropriate behaviour, attitude and skills to enable them to remain both safe and legal when using the internet and related technologies. With this in mind, our Computing curriculum has focused online safety lessons and core online safety themes are embedded throughout the academic year.

This Online-Safety Policy has five key sections:

- Roles and Responsibilities
- Managing Pupils' Access to Technology
- Teaching and Learning
- Communications policy
- Information and Links.

The school's online safety policy shall operate in conjunction with other policies including the Safeguarding Policies.

All staff and shareholders must abide by acceptable use agreements.

Roles and Responsibilities

Governing Body

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

- Review this policy annually and in response to any online safety incident to ensure that: the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- 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 online safety within the school. The day-to-day management of this shall be delegated to the computing lead. The Headteacher shall ensure that:

- Online safety training throughout the school is planned, up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team, governing body and parents.

- The designated online safety leads (computing lead and DSLs) have had appropriate training in order to undertake their day-to-day duties, including following up on-line safety alerts.
- All online safety incidents are dealt with promptly and appropriately.

Computing Lead

Reporting to the Headteacher, the computing lead is responsible for the day-to-day delivery of online safety learning activities throughout the school. The computing lead shall:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher and Governing body on all online safety matters.
- Engage with parents and the school community on online safety matters at school and/or at home.
- Liaise with the Local Authority, IT technical support and other agencies as required.
- Provide support with any online safety issues raised via a Concerns Log
- Support the Senior Leadership Team in the completion of the online safety Audit (Appendix A)
- Carry out regular checks of the internet filtering software

IT Technical Support Staff

Reporting to the Headteacher and the computing lead, the IT Technical Support Staff are responsible for delivery of effective, secure and safe IT Solutions for the school. The Technical support staff are responsible for:

- Ensuring any technical online safety measures in school (e.g. Internet filtering software) are fit for purpose and operating correctly through liaison with the Local Authority.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the computing lead, DSL(s) and Headteacher.
- Ensuring Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Ensuring Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Ensuring Passwords are applied correctly to all staff.
- Monitoring and reporting of documents stored on internal systems, internet and email use for both staff and pupils and report any inappropriate action to the Headteacher.
- Ensuring the IT System Administrator password is to be changed regularly.

All Staff

Staff shall ensure that:

- All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Headteacher or computing lead.
- Any online safety incident is captured within CPOMs and reported to the Headteacher or in his/her absence, to the DSLs or computing lead. If you are

unsure the matter is to be raised with the computing lead or the Headteacher to make a decision.

- Use of technology in lessons, in particular the use of the internet, has been checked to ensure age-appropriate content.
- Where appropriate, staff should ensure they feel adequately informed to be able to deliver online safety lessons to students.

All Pupils

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services shall be dealt with in accordance with the behaviour policy. Students are also made aware of the Computing Charter (Appendix B), highlighting their rights and responsibilities.

Online safety is embedded into our curriculum; students shall be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware of 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 support parents to help them gain the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters and workshops, the school will keep parents up to date with new and emerging online safety risks, and will involve parents in strategies to ensure that students are empowered to make informed decisions. It shall be made clear to Parents that the school needs rules in place to ensure that their child can be properly safeguarded. As such, parents shall sign the student Acceptable ICT Use Policy before any access can be granted to school ICT equipment or services.

Managing Pupils' Access to Technology

Mill Hill uses a range of devices including PC's, laptops and iPads.

Use of the Internet

Internet use is part of the statutory curriculum and a necessary tool for staff and pupils. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use shall be granted to: staff upon signing the staff Acceptable Use Policy and pupils upon signing and returning their acceptance of the Acceptable Use Policy. Students must request permission before using the internet and only access sites approved by staff.

The school's Internet access is provided by Hampshire County Council (HCC) and includes filtering appropriate to the age of pupils. An additional filtering set is available on staff devices to allow access to additional resources e.g. YouTube. There is no access to social media sites e.g. Facebook, Instagram. Note: There is still a small risk that inappropriate material may occasionally get through filters. This is managed through teachers' online safety training and pupils are taught what to do if this happens. IT Support, working closely with HCC, is responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher. If staff or pupils discover an unsuitable site, it must be reported to the computing lead (or Headteacher in case of their absence), who in turn will alert Rocket who will take swift and suitable action.

Online Learning Platforms/Apps (Purple Mash, TT Rockstars, EdShed)

Where pupils have been provided with a school learning platform account the school reserves the right to monitor all communications on the platform.

Pupils must not reveal personal details of their learning platform account to anyone other than their teachers and parents.

Pupils should avoid sending messages with lots of repetition or slang as these make it harder for others to read and help each other.

If these apps are misused, the class teacher with the support of the computing lead, will address this with the parent and child by reviewing the Acceptable Use Policy.

Continued incidents could result in removal of access.

Managing Email Use

- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published Work and the School Website

Websites can celebrate pupils' work, promote the school and publish resources for projects. The contact details on the website will be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published. The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images

Still and moving images and sounds add liveliness and interest to a publication and celebrates pupils' achievements. Nevertheless, the security of staff and pupils is paramount.

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name.
- Pupils' full names will not be used anywhere on the Web site or School Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Parents are instructed not to upload any photos taken during performances or assemblies to social media.

Social Networking

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited school control.

The school operates two strands, which may seem at first to be contradictory, encouraging pupils to observe legal restrictions and educating them to make good choices that will keep them safe if they choose to ignore site age restrictions

- The school will block access to social networking sites for both pupils and staff inside school.
- Pupils are advised by the school not to join social networks until they are legally entitled to do so. Most social networks sites have a 13-year age limit or older. Parents are also encouraged not to allow pupils to sign up underage at home as

immature users often make poor decisions that leave them open to the possibility of cyberbullying, loss of security and paedophile grooming.

However, the school recognises its responsibility to educate pupils to make safe choices if they choose to ignore age restrictions whilst at home and in light of this pupils are advised to:

- Never give out personal details of any kind which may identify them and / or their location.
- Recognise that any photo shared is beyond the control of the user who has shared it and may be used or adapted for purposes that the user would not wish for. This could include cyberbullying, harvesting details about their home in preparation for burglary electronic manipulation/morphing of the photo.
- Keep a locked down profile which doesn't identify them as a school child
- Recognise that social networks can never be totally safe as the user cannot manage what other members of the network do with information shared.

Assessing Risks

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will need to address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or school learning platform. Neither the school nor HCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will regularly audit Computing use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

Handling Online Safety Complaints

A minor transgression of the rules may be dealt with by the teacher. Other situations could potentially be serious and a range of sanctions are required, linked to the discipline policy. Potential child protection or illegal issues must be referred to the school Designated Safeguarding Lead or Computing lead. Advice on dealing with illegal use could be discussed with the local Police Youth Crime Reduction Officer.

- Complaints of Internet or learning platform misuse by pupils will be dealt with by a senior member of staff.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions will be applied appropriately within the school's behaviour policy
- Staff will teach the importance of following the Acceptable Use of IT policy in class making links to the context.

Teaching and Learning

Why is it Important?

Internet use is a part of the statutory curriculum and a necessary tool for pupils. The National Curriculum for computing Sept 2014 states pupils should be taught to:

- understand computer networks including the internet; how they can provide multiple services, such as the world wide web; and the opportunities they offer for communication and collaboration
- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

These statements describe how pupils should both understand how the Internet works and be confident, competent, creative and safe users of these technologies.

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use will Enhance Learning

Developing effective practice in Internet use for teaching and learning is essential. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be 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.

Pupils will be Taught How to Evaluate Internet Content

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop skills in selection and evaluation. Information received via the Internet, e-mail or text message requires good information handling skills. In particular, it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read. A whole curriculum approach may be required.

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher. To encourage self-censorship, the school operates a no blame policy where pupil's first response to materials that make them feel uncomfortable is to report them to their teacher.

If pupils are learning at home and encounter inappropriate materials, we would encourage parents to take the same no blame approach if it is reported to the parent straight away. If materials are linked unwittingly through the school's learning platform, we would ask parents and pupils to report this to the child's teacher or the school office so this can be rectified. All effort is made to avoid this happening but on rare occasions links or web pages are defaced or changed which can cause materials to become inappropriate.

More often, pupils will be judging reasonable material but will need to select relevant sections. Pupils are taught research techniques including the use of search engines and are encouraged to question the validity, currency and origins of information. Key information handling skills include establishing the author's name, date of revision and whether others link to the site. Pupils should compare web material with other sources.

Effective guided use also reduces the opportunity pupils have for exploring unsavoury areas.

Mill Hill will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Cyberbullying

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. 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. Cyber bullying is part of our planned computing curriculum (cross referencing with the PSHE curriculum) where all aspects of online safety for primary children are delivered. All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of our annual safeguarding training.

The school also sends information 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 Headteacher and 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.

Communications Policy

Introducing the online safety policy to pupils

Online safety rules are shared before any use of technology in lessons and all networked rooms in Mill Hill Primary Schools. Pupils will be informed that network and Internet use will be monitored. Each half term there will be a dedicated opportunity where every pupil will be taught about keeping themselves safe while they are online at an age-appropriate level. A module on responsible internet use will be included in the PSHE Curriculum covering both home and school use.

Staff and the online safety policy

All staff will be given the school online safety policy and its importance explained. Staff should be aware that Internet traffic can be monitored by the Head Teacher and traced to the individual user. Discretion and professional conduct are essential. Staff development in the safe and responsible internet use, and on school internet policy will be provided as required.

Enlisting parents' support

Parents' and carers' attention will be drawn to the online safety policy in newsletters, via parent mail and on their school's website.

Internet issues will be handled sensitively to inform parents without undue alarm.

By signing the Home School Agreement annually, parents and carers are agreeing to the acceptable use of this policy on behalf of themselves and their child(ren).

A partnership approach with parents is encouraged. This can include information at parents' evenings and suggestions for safe home Internet use.

Further Information and Links

Education for a Connected World

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS Education for a Connected World .pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf)

Project Evolve (Online Safety Teaching Resources)

<https://projectevolve.co.uk/>

Think U Know (CEOP Education program to support with protecting children from online sexual abuse)

<https://www.thinkuknow.co.uk/>

PEGI (Information about game suitability)

<https://pegi.info/app>

NSPCC (Support for parents keeping safe online)

<https://www.nspcc.org.uk/keeping-children-safe/online-safety/>

Childnet (Helpful information and guidance on a range of key online safety topics)

<https://www.childnet.com/>

Google Safety Centre

https://safety.google/intl/en_uk/families/

Appendix A

Online safety Audit

To be reviewed annually.

Does the school have an Online Safety Policy that complies with DfE guidance?	Y/N
Date of latest update:	
The policy was agreed by Governors on:	
The policy is available for staff	Y/N
The policy is available for parents	Y/N
The Designated Safeguarding Lead is:	
The Computing Lead responsible for leading online safety is:	
Has Online safety training been provided for staff?	Y/N
Has online safety training been provided for students?	Y/N
Do staff sign an acceptable ICT use agreement?	Y/N
Do parents sign and return the Computing Charter to say that their child will comply with the school online safety rules?	Y/N
Have Online safety rules been set for students?	Y/N
Are these rules displayed in school? ICT suite; classrooms	Y/N
Internet access is provided by an approved educational internet service provider and complies with requirements for safe and secure access.	Y/N

Mill Hill Primary School

Staff, Governor, Volunteer and Visitor Acceptable Use Agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of technology. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school Computing lead.

- I will only use the school's email / Internet / devices and any related technologies for professional purposes.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS, Target Tracker) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware or software without permission from the Computing Lead.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will not use the school's technology to promote private businesses, unless that business is directly related to the school.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent or carer.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of technology.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature Date
.....

Full Name
(printed)

Job title

KS2 Pupil Acceptable Use Agreement

Computing Charter

Completed every September.

These rules will be discussed as a class before the class sign them.

Acceptable Use of the School's Technology and Internet Mill Hill Computing Charter	
Name of Pupil: Class:	 Mill Hill PRIMARY SCHOOL
I will read and follow the rules in the acceptable use agreement policy. When I use the school's ICT systems (like computers) and get onto the internet in school I will: - Always use the school's ICT systems and the internet responsibly and for educational purposes only - Only use them when a teacher is present, or with a teacher's permission - Keep my username and passwords safe and not share these with others - Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carers - Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others - Always log off or shut down a computer when I'm finished working on it I will not: - Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity - Open any attachments in emails, or follow any links in emails, without first checking with a teacher - Use any inappropriate language when communicating online, including in emails - Log in to the school's network using someone else's details - Arrange to meet anyone offline without first consulting my parent/carers, or without adult supervision If I bring a personal mobile phone or other personal electronic device into school: - I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission - I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	
<i>Signed (pupil):</i>	<i>Date:</i>
<i>Signed (parent):</i>	

EYFS and KS1 Pupil Acceptable Use Agreement

Computing Charter

Completed every September.

These rules will be discussed as a class before the class sign them.

Acceptable Use of the School's Technology and Internet Mill Hill Computing Charter	
Name of Pupil: Class:	 Mill Hill PRIMARY SCHOOL
When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Ask a teacher or adult if I can do so before using them • Only use websites that a teacher or adult has told me or allowed me to use • Tell my teacher immediately if: - o I click on a website by mistake - o I receive messages from people I don't know - o I find anything that may upset or harm me or my friends • Use school computers for school work only • Be kind to others and not upset or be rude to them • Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly • Only use the username and password I have been given • Try my hardest to remember my username and password • Never share my password with anyone, including my friends • Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent • Save my work on the school network • Check with my teacher before I print anything • Log off or shut down a computer when I have finished using it I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	
Signed (pupil):	Date:
Signed (parent):	