Mill Hill
EDUCATION GROUP

Online Safety Policy

Instilling values, inspiring minds

Mill Hill
EDUCATION GROUP

Instilling values,
inspiring minds.

Online Safety Policy

Contents

Appendices

1. Introduction

Mill Hill Education Group (the 'Group') is the trading name of The Mill Hill School Foundation. It is a group of independent mainstream Schools which together educate girls and boys aged 6 months to 19 years. It currently comprises:

Senior Schools (Day and Boarding)
Mill Hill School
Mill Hill International
Cobham Hall
Heathfield School

Pre-Preparatory/Preparatory Schools (Day)
Grimsdell, Mill Hill Pre-Preparatory School*
Lyonsdown School*
Keble Prep School*
St Joseph's in The Park*
Belmont, Mill Hill Preparatory School

All Through Schools
Abbot's Hill School (age 6 months to GCSE)*
Kingshott School (age 3 to GCSE)*
Westbrook Hay School (age 3 to GCSE)*
*Schools with EYFS provision

This Policy applies to all Group Schools (including Early Years Foundation Stage (EYFS) settings. This Policy is published on the Schools' websites and is available in hard copy on request. The term 'Schools' in this Policy shall refer to each of the Group Schools, as appropriate.

The Mill Hill School Foundation is a Registered Charity. Both the Mill Hill School Foundation and Mill Hill School Enterprises are Companies Limited by Guarantee, employing both teaching and non-teaching staff. Legal responsibility rests with the Companies acting by the Court of Governors. The Head Teachers have day to day responsibility for the management of the Schools and the care of their Pupils.

The Group recognises the acceleration of the capabilities and widespread use of online technology in education has been significant in recent times. While presenting opportunities for research and education, internet enabled technology can present significant risks to children and young people. Keeping Children Safe in Education (**KCSIE**) states "Children are at risk of abuse and other risks online as well as face to face".

2. Aims, Objectives and Scope of the Policy

It is the duty of the Group Schools to ensure that every Pupil in their care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for learning and communication that can be used to enhance the curriculum, challenge Pupils, and support creativity and independence. Using IT to interact socially and share ideas can benefit everyone in the Group community, but this use can also pose great risks to young people. This Policy applies to all members of the School communities, including Staff, Pupils, Parent/s/Guardian/s/Carer/s, Governors and Visitors who have access to and are users of the Schools' IT systems.

The internet is used in Group Schools to raise educational standards, to promote Pupil achievement, to support the professional work of Staff and to enhance the Group's management functions. We want to equip our Pupils with all the necessary IT skills that they will need to enable them to progress confidently into a professional environment when they leave school.

In order to achieve this objective, we educate our Pupils on online safety issues, teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving Pupils in discussions regarding online safety and listening to their fears and anxieties as well as their thoughts and suggestions. Our Pupils are taught how to stay safe in the online environment, how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse, radicalisation and identity theft.

It is important that the use of the Internet and IT is seen as a responsibility and that Pupils, Staff, Parent/s/Guardian/s/Carer/s and Governors use appropriately and maintain good practice online. It is important that all members of the Group communities are aware of the dangers of using the internet and how they should conduct themselves online.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of the Group Schools include:

- Websites.
- Email and instant messaging.
- Blogs, forums and chat rooms.
- Mobile internet devices such as smart phones and tablets.
- Social networking sites.
- Music/video downloads.
- Gaming sites and online communities formed via games consoles.
- Instant messaging technology via SMS or social medica sites.
- Video calls.
- Podcasting and mobile applications.
- Virtual and augmented reality technology; and
- Artificial intelligence.

We know that some adults and young people may attempt to use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

A 'duty of care' is placed upon any person working with children. Educating all members of the Group communities on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This Policy aims to be an aid in regulating IT activity within the Group and provide a good understanding of appropriate IT use that members of the Group communities can utilise as a reference for their conduct online both inside and outside of school hours. Online safety is a whole-Group issue and responsibility.

The Group is conscious of its additional responsibilities to monitor the use of Digital Technology by its Boarding Pupils. The Designated Safeguarding Leads and Heads of Boarding for Mill Hill School, Mill Hill International, Cobham Hall and Heathfield School have joint overall responsibility for the online safety of pupils who Board. Boarding Pupils are obliged to comply with the provisions of the Boarding Handbook which contains specific guidance on Online Safety. The relevant section is annexed to this Policy in Appendix 1.

This Policy is implemented to protect the interests and safety of the Group's School communities. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. The Policy covers both fixed and mobile internet devices provided by the Group (such as Personal Computers, laptops, webcams, tablets, whiteboards, digital video equipment, etc); as well as all devices owned by Pupils and Staff brought onto School/Group premises (personal laptops, tablets, wearable technology e.g. smart phones and watches, etc), and is also applicable when Pupils are online in the home environment, for example when accessing remote learning.

Rules relating to the Group Code of Conduct when online, and online Safety Guidelines, are displayed around all Group Schools. Online safety is integrated into the Curriculum in any circumstances where the Internet or technology is being used, and during PSHE lessons where personal safety, responsibility, and/or development are being discussed. The Group holds events for Parent/s/Guardian/s/Carer/s on Internet Safety and includes advice on Online Safety, and in its Safeguarding Bulletins which are circulated to Governors, Parent/s/Guardian/s/Carer/s and Staff.

This Policy should be read in conjunction with the following Policies/Guidance for further clarity.

- Safeguarding and Protecting the Welfare of Pupils Policy.
- Acceptable Use of IT Policy/Agreement (Staff and Governors).
- Acceptable Use of IT Policy/Agreement (Pupils).
- Artificial Intelligence Policy.
- Anti-Bullying Policy.
- Promoting Positive Behaviour Policy.
- Staff Code of Conduct.
- Expectations and Standards Guidance (Mill Hill School and Mill Hill International).
- Boarding Handbook (Mill Hill School, Mill Hill International, Cobham Hall, and Heathfield School).
- PSHE and Relationships and Sex Education (PSHE and RSE) Policy.
- Educational Visits Policy.
- Data Protection Policy.
- Data Privacy Notice.
- Equality, Diversity and Inclusion Policies (Staff, and Pupils).
- Whistleblowing Policy.
- Prevent Strategies and Procedures.
- DfE Guidance on Teaching Online Safety in Schools (June 2019, updated Jan 2023).
- Keeping Children Safe in Education 2025 (KCSIE).
- UKCIS Education for a Connected World Framework (June 2020).
- DfE Advice on Sharing nudes and semi-nudes, advice for education settings 2024.
- Early Years Foundation Stage Statutory Framework 2025.
- Local Authority (Barnet, Berkshire, Enfield, Kent or Hertfordshire) Safeguarding Children Partnership Procedures.

3. Importance

The Group acknowledges the provisions of KCSIE which states: “Technology is a significant component in many safeguarding and wellbeing issue”. The internet and social medial have made information more accessible, but they've also amplified the spread of fake news - both misinformation (the unintentional spreading of false or misleading content) and disinformation (the deliberate creation and spread of false or misleading content, such as fake news). These forms of false content pose significant risks, particularly to children and vulnerable individuals, who may lack the skills to evaluate credibility. The impact includes emotional distress, confusion, and increased susceptibility to harm from misleading online content.

Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Technology can often provide a platform which facilitates child sexual exploitation, radicalisation, and sexual predation. The Group employs an effective approach to online safety therefore empowering each Group School to protect and educate their whole school community in the use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

In designing this Policy, the Group Schools have collectively considered the "4Cs" outlined in **KCSIE** (Content, Contact, Conduct and Commerce) as the key areas of risk. However, it is recognised that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some Pupils may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology whilst at School. The improper use of mobile technology by Pupils in or out of School, will be dealt with in accordance with the individual Group Schools' Positive Behaviour Policies and/or the Group Safeguarding and Protecting the Welfare of Pupils Policy as is appropriate in the circumstances.

The breadth of issues classified within online safety is considerable, but can be categorised in terms of risk as follows:

- **Content**: being exposed to illegal, inappropriate or harmful content, for example pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **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**: personal online behaviour that increases the likelihood of, or causes, harm: for example, 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**: being exposed to risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

4. -Roles and Responsibilities in Relation to Online Safety

All Staff, Governors and Visitors have responsibilities in accordance with the Group Safeguarding and Protecting the Welfare of Pupils Policy to protect pupils from abuse and make appropriate referrals. The following roles and responsibilities must be read in line with this Policy.

4.1 The Governing Body

In accordance with KCSIE , the Court of Governors has overall leadership responsibility for safeguarding as outlined in the Group Safeguarding and Protecting the Welfare of Pupils Policy and holds online safety as a central theme in their whole-setting approach to safeguarding. It is essential that Pupils are safeguarded from potentially harmful and inappropriate online material. Their approach to online safety empowers the Group to protect and educate Pupils and Staff in their use of technology, with mechanisms in place to identify, intervene in, and escalate any concerns where appropriate.

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the Policy by reviewing online incidents and monitoring reports. Online safety falls within the remit of the Governor responsible for Safeguarding.

The role of the Online Safety Governor will include:

- Ensuring an Online Safety Policy is in place, reviewed annually and/or in response to an incident and is available to all stakeholders.
- Ensuring that each Group School has a Designated Safeguarding Lead (DSL) with responsibility for online safety, who has been trained to a level of knowledge which is relevant to the School, up to date and progressive.
- Ensuring that Safeguarding Training for Staff, including Online Safety Training, is integrated and considered as part of the whole school Safeguarding approach. All Staff must be aware of the Group Procedures and Policies that must be followed in the event of any abuse or suspected breach of online safety in connection to their School.
- Ensuring that pupils are taught about Safeguarding, including Online Safety.
- Ensuring that Procedures for the safe use of IT and the Internet, including appropriate Online Filtering and Monitoring systems, are in place and adhered to. (For details of Group Schools' Monitoring and Filtering Products please refer to Appendix 4).
- Holding the Head for each Group School and Staff accountable for online safety

4.2 Head and Senior Leadership Team/Senior Management Team

The Heads of each Group School has a duty of care for ensuring the safety (including online safety) of members of their School community though the day-to-day responsibility for online safety will be delegated to the Designated Safeguarding Leads (DSLs), who have also been appointed as Online Safety Coordinators. Any complaint about Staff misuse of technology in any of the Group Schools must be referred to the Head of the relevant School as a 'Safeguarding Issue' involving a member of Staff, for Central Support Staff a referral must be made to the Director of Finance and Resources.

The role of the Heads of each Group School will include:

- Ensuring access to Induction and training in Online Safety Practices for all users.
- Ensuring all Staff receive regular, up to date training.
- Ensuring appropriate action is taken in all cases of misuse.
- Working with the Group IT Director to ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensuring that Pupil or Staff personal data, as recorded within a Group School Management System and sent over the Internet is secured.
- Working in partnership with the Department for Education (DfE) and the Group IT Director to ensure systems to protect Pupils are appropriate and managed correctly.
- Working with the Group IT Director to ensure the IT system is reviewed regularly regarding security and that virus protection is installed and updated regularly.

4.3 Designated Safeguarding Leads (DSLs)

The Designated Safeguarding Leads (DSLs) for each Group School are acknowledged as having overall responsibility for online safeguarding within their School including online filtering and monitoring. The DSLs and Senior Leadership Teams follow all Government legislation and guidance regarding online safety to ensure their Pupils understand how to stay safe and behave online as part of existing Curriculum requirements.

The DSLs role includes:

- Being able to understand the unique risks associated with online safety, including the additional risks faced by pupils with SEND.
- Ensuring the Online Safety Policy is upheld at all times, working with the Head, Senior Leadership Team and IT Staff to achieve this aim.
- Taking appropriate action if in receipt of a report that engages this Policy relating to activity that has taken place online.
- Leading on safeguarding, including Online Safety, meetings.
- Overseeing filtering and monitoring of online systems and sharing any disclosure, report or suspicion of improper use of their School IT with the Head and Group Director of IT.
- Liaising with Staff (especially Pastoral Support Staff, School Nurses, IT and SENDCOs on matters of safety and safeguarding, including online and digital safety.
- Working in partnership with the DfE and the Internet Service Provider and Group IT Director to ensure systems to protect pupils are reviewed and improved.
- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments.
- Reporting to Senior Leadership/Management Team and/or Head of their School
- Liaising with the nominated member of the Governing Body and their Head to provide an Annual Report on Safeguarding, which includes online safety.
- Co-ordinating the training and workshops for Pupils, Staff, Governors Parents, Guardians and Carers to improve understanding of all aspects of online safety.
- Keeping up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (DfE), KCSIE, ISI, the CEOP (Child Exploitation and Online Protection), Childnet International, NSPCC, and the Local Safeguarding Children Procedures (LSCP) for Barnet, Berkshire, Enfield, Hertfordshire, and Kent Local Authorities.

The Designated Safeguarding Leads in each Group School are as follows:

Mill Hill School	:	Jade Boyle
Mill Hill International	:	Suchita Prakash
Cobham Hall	:	Suzanne Carney
Heathfield School	:	Claire Huyton
Belmont, Mill Hill Prep School	:	Kaarin Scanlin
Grimsdell, Mill Hill Pre-Prep School	:	Hannah Holwerda
Keble Prep	;	James Fleet
Lyonsdown School	:	Rittu Hall
St Joseph’s in The Park	:	Nicole Welsh
Kingshott School	:	Rhian Burrows
Abbot’s Hill School	:	Claire King
Westbrook Hay School	:	Samantha Taylor

Other:

The Group IT Director	:	Firas Al-Fakhri

The Designated Member of the Governing Body responsible for Online Safety is Nigel Taylor (Governor responsible for Safeguarding). He can be contacted c/o Clerk to the Court of Governors at governance@millhill.org.uk

The Director of Safeguarding for the Group is Mrs Jane Morris. She can be contacted at: Jane.morris@mhsFoundation.uk

4.4 Group IT Director/Technical Staff

IT Staff have a key role in maintaining a safe technical infrastructure at each Group School and keeping abreast with the rapid succession of technical developments. They are responsible for the security of the Schools' hardware system, its data and for training each Group's teaching and administrative Staff in the use of IT. They monitor the use of the internet and emails, maintain content fillers, and will report inappropriate usage to the Group Director of IT and Online Safety Coordinator of the respective School.

The Group IT Director is responsible for ensuring:

- That the Group's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the Group meets required online safety technical requirements and any relevant body online safety policy/guidance that may apply.
- The Group IT Director is invited to DSL meetings on a termly basis.
- That users may only access the networks and devices through a properly enforced Password Protection Policy.
- This Online Safety Policy, together with the Group Schools' approach to monitoring and filtering is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- That he keeps up to date with online safety technical information to effectively carry out the online safety role and to inform and update others as relevant.
- That the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Head of the relevant School or the Director of Finance and Resources or the DSL for investigation/action/sanction.
- That monitoring software/systems are implemented and updated as agreed in Group Policies.
- That the Group's IT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.

4.5 Teaching and Support Staff

All Staff as part of pre-start employment onboarding, and thereafter annually, review all relevant Group Policies via the VWV Policy Tracker. All Staff are required to sign and return the Acceptable Use of IT Policy/Agreement (Staff and Governors) before accessing Group School's systems. As with all issues of safety at the Group Schools, Staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

All Staff must read and understand this Online Safety Policy and enforce it in accordance with direction from the DSL and/or the Head/member of the Senior Leadership Team as appropriate.

Group staff are expected to:

- Read and follow the provisions of this Policy.
- Read and Agree to the Acceptable Use of IT Policy/Agreement (Staff and Governors).
- Attend training sessions organised by the Group to promote online safety.

- Report to the DSL of their School (in respect of Pupils) or the Head of their School (in respect of other members of Staff) if they become aware of misuse or attempted misuse of Digital Technology within the Group.

4.6 Pupils

Pupils must report any accidental access to materials of a [violent or sexual nature or that are otherwise, inappropriate] to the DSL/Online Safety Coordinator/appropriate teacher. Deliberate access to any inappropriate materials by a Pupil will be dealt with under the individual Group School's Behaviour Policy. Pupils should be aware that all internet usage via their School's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the Group School's filtering system. If this causes problems for schoolwork/research purposes, Pupils should contact the Online Safety Coordinator/ IT Staff for assistance.

Pupils are expected to:

- Read and follow the provisions in this Policy.
- Follow the Group's Acceptable Use Guidance for Pupils relating to the use of digital technology and accessing the Group Wi-Fi.
- Exercise their responsibility to speak out when they believe that their School's systems are being abused in any way.

4.7 Parents, Guardians and Carers

The Group believes that it is essential for Parent/s/Guardian/s/Carer/s to be fully involved with promoting online safety both in and outside of School. The Group regularly consults and discusses online safety with Parent/s/Guardian/s/Carer/s and seeks to promote a wide understanding of the benefits and risks related to internet usage and to reinforce the importance of children being safe online.

Parent/s/Guardian/s/Carer/s bear full responsibility for ensuring their child's conduct online outside of School hours, irrespective of whether the device in use is personally owned or issued by the School. Parent/s/Guardian/s/Carer/s must take all reasonable steps to prevent the unlawful, inappropriate, or harmful use of technology on any device utilised by their child, with particular regard to devices provided by the School or designated for educational purposes.

Group School will contact Parent/s/Guardian/s/Carer/s if it has any concerns regarding a Pupil and/or Pupils' behaviour in this area and likewise it hopes that Parents, Guardians or Carers will feel able to share any concerns with the School.

It is important for Parent/s/Guardian/s/Carer/s to be aware of what their children are being asked to do online, including the sites the School will ask them to access and who they will be asked to interact with online.

They are therefore advised to:

- Read any Group online safety guidance for Parent/s/Guardian/s/Carer/s that is circulated from time to time.

- Attend Online Safety sessions and training sessions organised by the Group.

5 Education and Training

5.1 Staff: Awareness and Training

As part of their Induction, all new Teaching Staff receive information on online safety, including their School's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Online Safety Policy.

All Staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the Group's Online Safety behaviours.

Group School's must ensure that:

- New teaching Staff receive information on online safety and acceptable use as part of their induction.
- All teaching Staff receive regular information and training on online safety issues in the form of targeted training and internal briefings and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. This includes updated information regarding online filtering and monitoring responsibilities and procedures in their respective School.
- Staff training in Group Schools is logged centrally.
- All Staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following School online safety procedures. When Pupils use School computers, Staff should make sure they are fully aware of the Agreement they are making to follow the School's Acceptable Use Guidelines.
- Teaching Staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the School community.
- All incidents relating to online safety should be reported to the DSL.

5.2 Pupils: The Teaching of Online Safety

The Group delivers age, and stage of development-, appropriate online education through the tutor programme, PSHE, assemblies, discussion, talks and the academic curriculum. These are planned and delivered using relevant guidance, tools and resources.   This education aims to ensure that all Pupils develop the underpinning knowledge and behaviours required to navigate the online world safely, in a way which suits their age and ability. Teaching Staff assist Pupils achieve this by reinforcing the Group's fundamental values.

The through-Group Curriculum focuses on the following:

- IT and online resources are used increasingly across the Curriculum. The Group believes it is essential for online safety guidance to be given to Pupils on a regular and meaningful basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

- The Group Schools provide opportunities to teach about online safety within a range of Curriculum areas (as above), IT lessons, as well as informally when opportunities arise.
- At age-appropriate (and stage-of-development-appropriate) levels, and usually via PSHE, Pupils are taught to look after their own online safety.
- Enables Pupils to understand what acceptable and unacceptable online behaviour looks like
- Raise awareness of the possible online risks and help pupils make informed decisions about how to act and respond.
- Reinforce to all Pupils the importance of knowing how, when and where they can seek support if they are concerned or upset by something they see or experience online.
- Provide opportunities for Pupils, Parent/s/Guardian/s/Carer/s and Staff to have access to educational workshops, lectures and resources on the all aspects of online e- safety.
- Recognise the consequences of inappropriate online behaviour in line with the Group's Promoting Positive Behaviour Policy but also on their own digital footprint.
- Supporting Pupils to understand and follow this Policy and the Pupil Guidance which may be issued by each School regarding the acceptable use of digital technology and online safety.
- At age-appropriate points, Pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL (who is the Online Safety Lead) and indeed any member of Staff at the School.
- Pupils are also taught about relevant laws applicable to using the internet, such as data protection online safety, and intellectual property. Pupils are taught about respecting other people's information and images.
- Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the Groups' Anti-bullying Policy, which details the preventative measures and the Procedures that will be followed when the School discovers cases of bullying. Pupils should approach the DSL who is the School's Online Safety Lead or other members of Staff they trust, as well as Parents, Guardians Carers, Peers and other School Staff for advice or help if they experience problems when using the internet and related technologies.

Special one-off events and awareness days are held to raise the profile of online safety, namely on Safer Internet Day.

5.3 Pupils: Vulnerable Pupils

- The Group is aware that some Pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss. It may also include those children who have received multiple suspensions or are at risk of being permanently excluded.
- Each Group School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable Pupils.
- The Group Schools will seek input from specialist staff as appropriate, including the SENCO.

6. Cyberbullying

The Group, as with any other form of bullying, takes Cyber bullying, very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in each Group School's Promoting Positive Behaviour and Anti-Bullying Policies. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the Group community what is expected of them in terms of respecting their Peers, members of the Public and Staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does occur, the Group will:

- Take it seriously.
- Act as quickly as possible to establish the facts. It may be necessary to examine Group systems and logs or contact the service provider to identify the bully.
- Record and report the incident.
- Provide support and reassurance to the victim and support the perpetrator via the individual School's Promoting Positive Behaviour Policy.

7. The Threat of Online Radicalisation

The internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs such as extreme ideological views or the use of violence to solve problems.

In line with Prevent guidance, protecting children from the risk of radicalisation, the Group has a number of measures in place to ensure that pupils are safe from terrorist and extremist material when accessing the internet in school, and to help prevent the use of social media for this purpose:

- Website filtering and monitoring is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by Pupils.
- Pupils, Parent/s/Guardian/Carer/s and Staff are educated in safe use of social media and the risks posed by on-line activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found on the Educate Against Hate website (www.educateagainsthate.com), which is designed to equip Schools and College Leaders, Teachers. Parent/s/Guardian/Carer/s with the information, tools and resources they need to recognise and address extremism and radicalisation in young people, including in online issues.

8. Responding to Online Safety Incidents and Concerns

All members of the Group community will be made aware of the reporting procedure for online safety and safeguarding concerns regarding Pupil welfare including:

- breaches of filtering.
- youth produced sexual imagery (sexting).
- upskirting, cyberbullying, online sexual harassment (including cyberflashing - sending images of one's genitals to strangers online, which became a criminal offense on 31st January 2024).
- sextortion (individuals being forced into paying money or meeting another financial demand, after a
- person has threatened to release nude or semi-nude photos of them (this could be a real photo, or a fake image created of the victim by the person threatening its release) and illegal content.

The School requires Staff, Parent/s/Guardian/s/Carer/s, and Pupils to work in partnership to resolve online safety issues.

All members of the community must respect confidentiality and the need to follow the official Group School Procedures for reporting concerns. (For further detailed information please refer to the Group Safeguarding and Protecting the Welfare of Pupils Policy, Complaints Policy and Procedures, and Whistleblowing Policy. The Policies can be located on the Schools' websites.

After any investigations are completed, the School will debrief, identify lessons learnt and implement any Policy or Curriculum changes as required.

If the School is unsure how to proceed with an incident or concern, the DSL will seek advice from the Local Authority Safeguarding Team. Where there is suspicion that illegal activity has taken place, the School will contact the Local Authority Safeguarding Team or the Police using 101, or 999 if there is immediate danger or risk of harm.

Any allegations regarding a member of Staff's online conduct will be referred to the Head and discussed with the DSL/Online Safety Lead and the LADO (Local Authority Designated Officer) if necessary. Appropriate action will be taken in accordance with the Staff Code of Conduct and Safeguarding and Protecting the Welfare of Children Policies.

When made aware of concerns involving consensual and non-consensual sharing of, or the threat to the sharing of, nudes and semi-nude images and/or videos by children, Staff are advised to:

- Report any concerns to the DSL immediately.
- Never view, copy, print, share, store or save the imagery, or ask a child to share or download it – this may be illegal. If Staff have already viewed the imagery by accident, this will be immediately reported to the DSL.
- Not delete the imagery or ask the child to delete it.
- Not say or do anything to blame or shame any children involved.
- Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.
- Not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of Staff, the child(ren) involved or their, or other, Parent/s/Guardian/s/Carer/s. This is the responsibility of the DSL.

The DSL will respond to the concerns as set out in the non-statutory UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)

For further details regarding the procedures for responding to specific online incidents or concerns, please contact the DSL/Online Safety Lead in the School.

9. Monitoring and Filtering

The Group aims to provide a safe environment to learn and work, including when online. The Group will ensure that appropriate monitoring and filtering systems are in place when Pupils and Staff access School Systems and internet provision, in order that exposure to any risks can be reasonably limited. Filtering and monitoring are both important parts of safeguarding Pupils and Staff from potentially harmful and inappropriate online material, but must function without unreasonably impacting teaching and learning, in line with the DfE filtering and monitoring standards which were updated in May 2024.

Staff, Pupils, Parent/s/Guardian/s/Carer/s, Governors and Visitors should be aware that the Group School's monitoring and filtering systems apply to all users; all School owned devices and any device connected to the Schools' internet servers. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the monitoring and filtering systems will be dealt with under the Group Staff Code of Conduct Policy or the School's Behaviour Policy, as appropriate. (Details of Group School's Monitoring and Filtering Product currently in use may be found at Appendix 4.

9.1 The Group review our approach to monitoring and filtering regularly and assess the effectiveness of the current provision, any gaps, and the specific safeguarding needs of pupils (their age ranges, those who are at greater risk of harm for example those with SEND, or those with English as an Additional Language (EAL)) and staff. This happens annually (at the very least), or more often if circumstances dictate, such as when:

- A safeguarding risk is identified.
- There is a change in working practice, like remote access or BYOD (bring your own device).
- New technology is introduced.

Any checks to the Group's filtering provision are completed and recorded as part of the filtering and monitoring review process.

9.2 The Governors have overall strategic responsibility for meeting this requirement, and they have assigned day to day responsibility for the following to the Governor with specific responsibility for IT, the Heads and the Group IT Director:

- Procuring filtering and monitoring systems.
- Reviewing the effectiveness of the Group's provision.
- Overseeing reports.

9.3 They must also ensure that all Staff:

- Are appropriately trained for their role.
- Understand that it is everyone's responsibility to keep the online environment safe, including the effective use of monitoring and filtering.
- Follow the Staff Code of Conduct, all Policies, Processes and Procedures.
- Act on reports and concerns and record them appropriately.

9.4 The DSL has the lead responsibility for safeguarding and online safety, which includes overseeing and acting on:

- Monitoring and filtering reports.
- Safeguarding concerns.
- Checks to monitoring and filtering systems.

9.5 The IT Support Department has the technical responsibility for:

- Maintaining monitoring and filtering systems.
- Providing monitoring and filtering reports.
- Completing actions following concerns or checks to systems.

It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate Staff, such as the Senior Leadership/Management Team or the Designated Safeguarding Lead. The Group therefore reserves the right to regularly monitor and filter a Staff members/Pupil's use of the internet, social media and e-mail systems when at work or when using Group electronic equipment.

Such monitoring/filtering includes the right to read e-mails sent or received on electronic equipment provided by the Group or view photographic images captured on electronic equipment provided by the Group to check that the use by employees is in accordance with this Policy. In line with the Group's

Data Protection Policy and Data Privacy Notice, the DSLs in accordance with their Online Safety Coordinator role, and IT Staff will monitor the logs.

9.6 If any member of Staff has any concern about the effectiveness of the monitoring and filtering System they must report it to the DSL immediately in line with the Group Safeguarding and Protecting The Welfare of Children Policy.

All Staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They must report if:

- They witness or suspect unsuitable material has been accessed.
- They can access unsuitable material.
- They are teaching topics which could create unusual activity on the filtering logs.
- There is failure in the software or abuse of the system.
- There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks.
- They notice abbreviations or misspellings that allow access to restricted material.

9.7 The Court of Governors support the Senior Leadership/Management Team to review the effectiveness of monitoring strategies and reporting processes. Any incidents that are identified, are acted on with urgency and outcomes are recorded. Incidents could be of a malicious, technical, or safeguarding nature. Staff understand that in the first instance, they report their concerns to the DSL.

9.8 If it is discovered that any of the systems are being abused and/or that the terms of this Policy are being infringed, disciplinary action may be taken in accordance with the provisions of the Group's Disciplinary Policies and Procedures.

10. Online Safety Review

The DSLs of each Group School will regularly review its Online Safety Provision and Education as part of the annual Safeguarding Audit and may use tools such as Online 360 Degree Safe (www.360safe.org.uk) as part of such a review.

11 Security and Management of Information Systems

The Group is responsible for reviewing and managing the security of the computers and Internet networks and takes the protection of Group data and personal protection of our Group community very seriously. This means protecting the Group network, as far as is practicably possible, against viruses, hackers and other external security threats. The Group IT Director will review the security of the Group information systems and users regularly and virus protection software will be updated regularly at least annually,(or more regularly if circumstances dictate).

The Group implements the following safeguards to ensure the security of computer systems:

- Advising Staff that all personal data sent over the Internet should be encrypted.
- Making sure that unapproved software/apps are not downloaded to any Group devices. Alerts will be set up to warn users of this.
- Files held on the Group network will be regularly checked for viruses.
- The use of secure user logins and passwords to access the Group network will be enforced.
- Portable media containing school data or programmes will not be taken off-site.

- Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be **immediately** reported to the IT team.

For more information on data protection in the Group please refer to the Data Protection Policy or seek further advice from the Compliance Manager at compliance@millhill.org.uk.

12. Emails

The Group uses email internally for Staff and Pupils, and externally for contacting Parent/s/Guardian/s/Carer/s and is an essential part of Group communication. It is also used to enhance the Curriculum by:

- Initiating contact and projects with other Schools nationally and internationally.
- Providing immediate feedback on work, and requests for support where it is needed.

Staff and Pupils should be aware that Group email accounts should only be used for Group-related matters, i.e. for Staff to contact Parent/s/Guardian/s/Carer/s or Pupils, other members of Staff and other professionals for work purposes. This is important for confidentiality. The Group reserves the right to monitor emails and their contents but will only do so if it feels there is reason to.

12.1 Staff Use of Email and the internet

Staff should be aware of the following when using emails in the Group:

- Staff should only use official Group-provided email accounts to communicate with Pupils, Parent/s/Guardian/s/Carer/s. Personal Email accounts must not be used to contact any of these people.
- The Group permits the incidental personal use of email, the internet, social media and related types of electronic communication and information, and electronic equipment by a member of Staff if it is kept to a minimum and takes place substantially out of normal working hours.
- Staff should be aware that all personal interactions (email and internet) on a Group device are logged and may be monitored.
- Use must not interfere with an employee's work commitments, or those of others. If it is discovered that excessive periods of time have been spent on the internet or other electronic media provided by the Group, either in, or outside, working hours disciplinary action may be taken and internet access or use of electronic equipment may be withdrawn without notice at the discretion of the Head of the relevant Group School or the Director of Finance and Resources/Chief Executive Officer.
- Emails sent from Group accounts should be professionally and carefully written. Staff are always representing the Group and should take this into account when entering into any email communications.
- Where possible, Staff should avoid 'replying to all' or blindly forwarding emails they have received. Be selective in your email use.
- Staff must advise their Line Manager or a member of the Senior Leadership/Management Team if they receive any offensive, threatening or unsuitable Emails either from within the School or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in the Group.
- Using photographic material of any kind to bully, harass or intimidate others will not be permitted and will constitute a serious breach of discipline and may lead to dismissal.

12.2 Pupil Use of Email

Pupils should be aware of the following when using email in School, and will be taught to follow these guidelines through the IT Curriculum and in any instance where email is being used within the Curriculum or in class:

- In school, Pupils should only use Group-approved email accounts.
- Excessive social emailing will be restricted.
- Pupils should advise a member of Staff if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.
- Pupils must be careful not to reveal any personal information over email or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

Pupils will be educated through the PSHE curriculum to identify spam, phishing and virus Emails and attachments that could cause harm to the Group network or their personal account or wellbeing.

13. Safe Use of Digital and Video Images of Pupils

The development of digital imaging technologies has created significant benefits to learning, allowing Staff and Pupils instant use of images that they have recorded themselves or downloaded from the internet. However, Staff, Parent/s/Guardian/s/Carer/s and Pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, Staff will inform and educate Pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet (e.g., on social networking sites).

13.1 The School Website

The Group considers the Schools' website to be a useful tool for communicating our ethos and practice to the wider community. It is also a valuable resource for Parent/s/Guardian/s/Carer/s , Pupils, and Staff for keeping up to date with School and Group news and events, celebrating School and Group-wide achievements and personal achievements, and promoting School projects.

Any information published on the website will comply with good practice guidance on the use of such images and be carefully considered in terms of safety for the Group community, copyrights and privacy policies. No personal information relating to Staff or Pupils will be published, and details for contacting the Group will be for the relevant School office only.

13.2 Safe Use of a Pupil's Digital Images and Data

In accordance with the Data Protection Act 2018, images of Pupils and Staff will not be displayed in public, either in print or online, without prior consent. On admission to each Group School Parent/s/Guardian/s/Carer/s will be asked to sign a Photography Consent Form. For Pupils 13 and above their explicit consent is also required. The Group requests their consent to prevent repeatedly asking Parent/s/Guardian/s/Carer/s for consent over the school year, which is time-consuming for both Parent/s/Guardian/s/Carer/s and the Group. The Terms of Consent contained in the Photography

Consent Form will remain in force during the period of time a Pupil attends a Group School. Published images do not identify Pupils or put them at risk of being identified unless they or their Parent/s/Guardian/s/Carer/s consent. Pupils may be identified by their first name only.

Images published on the website must not be reused or manipulated. Only images created by or for the School/Group will be used in public and Pupils may not be approached or photographed while in School or undertaking School activities without the Group/school's permission.

The Group follows general rules on the use of photographs/videos of pupils:

13.2.1 By Parents, Guardians and Carers:

- Parent/s/Guardian/s/Carer/s and others are welcome to take digital images and videos of their children at School events for their own personal use, with consideration and courtesy for cast members or performers on stage and the comfort of others. Flash photography can disturb others in the audience or even cause distress for those with medical conditions; the Group therefore asks that it is not used at indoor events.
- Parent/s/Guardian/s/Carer/s are asked not to take photographs of other Pupils, except incidentally as part of a group shot, without the prior agreement of that Pupil's Parent/s/Guardian/s/Carer/s and publish them on any social media sites, or otherwise publish those images or videos
- Parent/s/Guardian/s/Carer/s should take care taken when taking photographs or videos to ensure that Pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Group Schools into disrepute (they should not be filmed backstage during productions or in changing rooms).
- The Group does not however agree to any such photographs or videos being used for any other purpose.
- The Group reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from any Parent/s/Guardian/s/Carer/s who does not follow these guidelines or is otherwise reasonably felt to be making inappropriate images.
- Parent/s/Guardian/s/Carer/s are reminded that copyright issues may prevent the Group from permitting the filming or recording of some plays and concerts. The Group will print a reminder in the programme of events where issues of copyright apply.
- At Grimsdell, Mill Hill Pre-Preparatory School, Parent/s/Guardian/s/Carer/s are not permitted to take photographs or use their mobile phones at any time around the School other than events described above.

13.2.3 By Pupils:

- The use of cameras or filming equipment (including on mobile phones or mobile action cameras, such as Go Pro cameras) is not permitted in toilets, washing or changing areas, nor should photography or filming equipment be used by Pupils in a manner that may offend, or cause upset.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- The Group recognises that consensual and non-consensual sharing (or threats to the sharing) of nudes and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or "sexting") by/of Pupils can be a safeguarding issue. All concerns will be reported to and dealt with by the DSL (or deputy). Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is

illegal which makes responding to incidents complex. (For further information, please see the Safeguarding and Protecting the Welfare of Pupils Policy.)

- The misuse of images, cameras or filming equipment by Pupils in a way that breaches this Policy, or any other Group Policy is always taken seriously, and will be dealt with under the relevant Policy as appropriate.

13.2.4 By the Group:

- Throughout the Group community we are proud to celebrate the achievements of our Pupils and therefore may want to use images and videos of our Pupils within promotional materials, or for publication in the media, such as local, or even national, newspapers covering School events or achievements. We will seek the consent of Pupils, and their Parent/s/Guardian/s/Carer/s where appropriate, before allowing the use of images or videos of pupils for such purposes.
- When a Pupil commenced their attendance at a Group School, they, or their Parent/s/Guardian/s/Carer/s would have signed a Photography Consent Form in relation to the use of images and videos of themselves or child. The Group Schools do not use images or videos of Pupils for any purpose where-prior consent has not been obtained.
- Staff and Volunteers are permitted to take digital and video images to support educational aims, but must follow this Policy concerning the sharing, distribution and publication of those images.
- Staff are encouraged to use Group issued equipment for the purposes of taking photographs/stills or video footage of pupils. With the exception of Early Years Foundation Stage (EYFS) Staff, personal devices may be used provided (a) the image taken is 'appropriate' and is in accordance with the Group's Storing and Use of Images Policy and (b) the image is removed from the device within 48 hours. Any such use should always be transparent, and Staff should be aware of those Pupils for whom consent has not been given (details may be obtained from the Marketing and Communications Department.). The resulting files from such recordings or taking of photographs must be stored in accordance with the Group's Procedures on Group equipment. If an existing local practice of an individual School is of a higher standard than the guidance detailed above, the local practice should continue to be adhered to.
- In the EYFS settings, teachers use several EYFS Online Learning Journals and Online Classroom Sharing Portals, for example Tapestry, Seesaw, Google Classroom and Atom. These Forums permit access. Parent/s/Guardian/s/Carer/s may not share photographs from this Forum. (Please contact the School for further information about obtaining the images). (Please refer to Appendix 2 for further details of School-specific information.

13.3 Complaints regarding the Misuse of Digital Images or Video

- Parent/s/Guardian/s/Carer/s should follow the standard School Complaints Procedure if they have a concern or complaint regarding the misuse of photographs/images/videos published by any Group School. Please refer to the Group Concerns and Complaints Policy, which can be found on the Group website for further information on the process to follow when making a complaint. Any issues or sanctions will be dealt with in accordance with the Safeguarding and Protecting the Welfare of Pupils Policy.
- Misuse of images/videos in any form by Pupils and others, will be dealt with in accordance with the Group School's Positive Behaviour Policy and/or the Anti-bullying Policy, according to the type of incident. Should there be an instance of Pupils sharing nudes and semi-

nudes of under-18s, which is illegal even with the individual's consent, the matter will be immediately referred to the DSL and the Head of the Group School.

14. Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging. These online Forums are the more obvious sources of inappropriate and harmful behaviour and where Pupils are potentially more vulnerable to content, contact and conduct behavioural issues. It is important that Group Schools educate Pupils so that they can make their own informed decisions and take responsibility for their conduct online. There are various restrictions on the use of these sites in School that apply to both Pupils and Staff.

14.1 Expectations:

- The expectations regarding positive, safe and responsible use of social media applies to all members of the Group community. The Group Schools will control Pupil and Staff access to social media whilst using school provided devices and systems on site.
- All members of the Group community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- Concerns regarding the online conduct of any member of the Group community on social media, should be reported to the Head and will be managed in accordance with our Anti-Bullying, Positive Behaviour, Safeguarding and Staff Code of Conduct Policies.

14.2 Staff Personal Use of Social Media:

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of Staff as part of Staff Induction and will be revisited and communicated via regular staff training opportunities. Further guidelines are found in the Staff Code of Conduct Policy.

14.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to Pupils as part of an embedded and progressive educational approach, via age-appropriate sites and resources.
- Pupils are expected not to engage in threatening, hurtful or defamatory online behaviour on social media platforms, in interactive online games or in the metaverse.

14.4 Official Group Use of Social Media

- The official use of social media sites, by the Group, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only. Official social media sites are suitably protected and, where possible, run and/or linked to/from the school website.
- Official social media use will be conducted in line with existing Policies, including Anti-Bullying, Data Protection, Safeguarding and the Staff Code of Conduct.

15. Use of Group and Personal Mobile Phones and Devices

While mobile phones and personal communication devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- Can make Pupils and Staff more vulnerable to cyberbullying.
- Can be used to access inappropriate internet material.
- Can be a distraction in the classroom.
- Are valuable items that could be stolen, damaged, or lost.
- Have integrated cameras, which can lead to child protection, bullying and data protection issues.
-

15.1 Use by Staff

- Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.
- School devices assigned to a member of Staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for schoolwork. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.
- School devices/cameras may be used for official photographs under the direction of the Head. These photographs must only be downloaded using the School's computers and not onto a personal, private computer. Please refer to the Staff Code of Conduct Policy for further details.
- Under no circumstances may Staff contact a Pupil, Parent/s/Guardian/s/Carer/s using a personal telephone number, email address, social media or messaging system.
- It should be noted that wherever possible, Staff will use Group-owned devices to capture images or videos, including live streaming (at Grimsdell, Mill Hill Pre-Prep School, this will always be the case). However, in the other Group Schools Staff may use personal mobile devices to take photographs of Pupils for social media purposes, **provided they comply with** any relevant Group Information Security Policy and that **ALL** images are only saved onto the relevant School's shared drive. If an existing local practice of an individual School is of a higher standard than the guidance detailed above, the local practice should continue to be adhered to.
- Personal cameras belonging to Staff and Volunteers are not to be used on Group School premises or School grounds at any time. Cameras on Staff owned mobile phones should not be used on School premises or School grounds at any time. No images may be taken of any Group School or any pupils using mobile phones or personal cameras.
- Personal mobile phones may be used in dedicated Staff areas or in class and teaching rooms only if the children are not present, or in the event of needing to use the Authenticator Application.
- Computing devices and wearables connected to the Group School networks must always use updated software to safeguard against critical zero-day security vulnerabilities. In special circumstances, should a device that is not supported need to be used on the network, a security risk assessment must be conducted and approved by the Security Group.
- Staff should not accept mobile phone calls during a lesson or when they are with Pupils. The only exception to this is if the Head or DSL calls a Staff member (usually only on Sports Days or on School trips, or if the School Office calls in similar circumstances). These calls will only be made in unusual or emergency (safeguarding) situations.
- Staff are advised to ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.

- If a member of Staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.
- The Group accepts no responsibility for, nor provides insurance against, theft, loss or damage of any staff personal property, including electronic equipment. All such equipment is brought onto the Group site at the owner's risk.

15.2 Use by Pupils

- Recent UK Government guidance regarding the use of mobile phones in Schools [Mobile phones in schools - February 2024 (publishing.service.gov.uk)] urges Schools to prohibit the use of mobile phones throughout the School day thereby ensuring the welfare of Pupils and maintaining an environment conducive to learning. This is likely to have the following beneficial effects:

- Enhanced Focus: Pupils can concentrate better on their studies without the distraction of mobile phones.
  (ii) Improved Social Skills: Pupils are more likely to engage in meaningful interactions during breaks.
- Reduced Cyberbullying: Limiting phone use can help decrease online harassment.
- Better Sleep Patterns: Reducing screen time during the day can improve sleep quality.
  Increased Academic Integrity: Removing phones during exams promotes honesty and fairness.
- The Group has clear Policies (age dependant) on the use of mobile and smart technology, reflecting the fact many Pupils now have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access increases the risk that some Pupils, whilst at school, are able to sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content.
- The Group recognises the importance of mobile phones as means of communication and safety when travelling to and from School. Where Pupils have smart phones, Parent/s/Guardian/s/Carer/s are responsible for ensuring that they have age-appropriate content filtering configured in the phone settings.
- These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.
- The Group Schools recognise that mobile devices are sometimes used by Pupils for medical purposes or as an adjustment to assist Pupils who have disabilities or special educational needs. Where a Pupil needs to use a mobile device for such purposes, the Pupil's Parents, Guardian or Carer should arrange a meeting with the SENDCo to agree how the School can appropriately support such use. The SENDCo will then inform the Pupil's teachers, the DSL, the IT Services Manager and other relevant members of Staff about how the Pupil will use the device at School. Medical monitoring devices, such as glucose monitoring devices which will require a medical assessment.
- Pupils are not permitted to bring in/use mobile phones or other digital devices in Pre-Prep settings, and Staff are not permitted to use their own mobile phones or other digital devices whilst at School (unless provided by the School for the purposes of teaching and learning whilst at school) in line with the provisions of EYFS regulations.
- Preparatory School Pupils are not permitted to use mobile phones or other digital devices in school. If Pupils bring in their mobile phones or other digital devices to School, these must be handed into the respective School Office/the Pupil's Form Tutor or Houseparent/designated location when they arrive onsite/at morning registration. The mobile phones/device will then

be returned to the Pupils during afternoon registration/at the end of the school day. Pupils are not permitted to take mobile phones and devices with connectivity to the internet on residential trips and visits.

- Senior Pupils may bring their mobile phones into School, but these must only be used in accordance with the respective School's guidance regarding their use. For example, at Mill Hill International Pupils will not be permitted to bring mobile phones into School during the School Day, apart from those day Pupils travelling in by public transport when they are acceptable for safety reasons (but who are required to hand them in to their Housemistress when they arrive). Other Group Schools have similar guidance which is communicated to Parent/s/Guardian/s/Carer/s
- There is separate guidance for Boarding Pupils at Mill Hill School, Mill Hill International, Cobham Hall and Heathfield School only, as to the use of their mobile phones and other devices at evenings and weekends. This is communicated to Parent/s/Guardian/s/Carer/s within relevant boarding documentation.
- Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- Any Pupil who brings a mobile phone or personal device (BYOD) into School is agreeing that they are responsible for its safety. Computing devices and wearables connected to the school network must always use updated software to safeguard against critical zero-day security vulnerabilities. The Group will not take responsibility for personal BYOD devices that have been lost, stolen, or damaged.
- Any concerns regarding Pupils use of mobile technology or Policy breaches will be dealt with in accordance with Group Policies, including Anti-Bullying, Safeguarding and Positive Behaviour.
- Staff may confiscate a Pupil's mobile phone or device if they believe it is being used to contravene Group Child Protection, Positive Behaviour or Anti-Bullying Policies. Mobile phones and devices that have been confiscated will be held in a secure place and released to Parent/s/Guardian/s/Carer/s.
- Pupil's mobile phones or devices may be searched by a member of the Leadership Team with the authority of the Head. (Please refer to the Anti-bullying Policy and the Group Searches Guidance document for further details). Content may be deleted or requested to be deleted if it contravenes Group Policies.
- Searches of mobile phone or personal devices will be carried out in accordance with the DfE 'Searching, Screening and Confiscation' Guidance: Searching, screening and confiscation at school - GOV.UK (www.gov.uk), July 2023, as outlined in the Group's Searches – Guidance and Protocol document.
- Appropriate sanctions and/or pastoral/welfare support will be implemented in line with Group Schools Promoting Positive Behaviour Policy.
- Concerns regarding policy breaches by Pupils will be shared with Parent/s/Guardian/s/Carer/s as appropriate.
- Where there is a concern that a child is at risk of harm, the Group will respond in line with the Safeguarding and Protecting the Welfare of Children Policy.
- If there is suspicion that material on a Pupil 's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

16. Livestreaming

Where the Group decides to permit the live streaming of an event or performance, the Group will seek the prior consent of Parent/s/Guardian/s/Carer/s or pupils (where applicable) to such live streaming, and any subsequent online accessibility to the performance.

17. Management of Applications which Record Children's Progress (Data and Images)

Group Schools use applications such as iSAMS, Engage, Arbor, Orah and Tapestry (EYFS) to track Pupil's progress and share appropriate information with Parent/s/Guardian/s/Carer/s (this list is not exhaustive). The Head of each School is ultimately responsible for the security of any data or images held of pupils. As such, they will ensure that tracking systems are appropriately risk assessed by the Group's IT Director and Compliance Manager prior to use, and that they are used in accordance with General Data Protection Regulation (GDPR) and Data Protection legislation.

To safeguard data:

- Only Group-approved apps and software will be used to access any pupil details, data and images, and these require secure sign ins, passwords and often two-factor authentication.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parent/s/Guardian/s/Carer/s will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

18. Managing Emerging Technologies including Artificial Intelligence

Technology is progressing rapidly, and new technologies are constantly emerging, including the introduction of Artificial Intelligence (AI),. While proposals for a new legislative and regulatory framework regarding Artificial Intelligence are at an early stage in the United Kingdon, generative AI tools such as Chat GPT are continuing to develop rapidly and be used increasingly widely across a range of contexts, including within education.

The Group assesses the potential risks of any new technologies before permitting their use in schools, carefully weighing these up with the potential educational advantages they may offer. The Group may inject AI into their practices, and by doing so, stays at the forefront of innovation, proactively monitoring and keeping abreast of emerging technologies. This approach allows the Group to promptly devise and implement suitable strategies to navigate the ever-changing technological landscape. (For further information, please refer to the Group AI and Acceptable Use of IT Policies).

19. Protecting Personal Data

The Group takes its compliance with the Data Protection Act 2018 seriously. Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation.

Staff and Pupils are expected to save all data relating to their work to their School Laptop/PC or to the Group School's central server/ All Staff devices should be encrypted if any data or passwords are stored on them. All removeable media (ISB, memory sticks, CDs or portable drives) taken outside of Group Schools or sent by post of courier must be encrypted before sending.

Staff may only take information offsite when authorised to do so and only when it is necessary and required in order to fulfil their role. No personal data of Staff or Pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provide by the School. Staff should be particularly vigilant about scam/phishing emails (and similar) which could seriously compromise the Group School's IT security and/or put at risk personal data (and other information) held by the Group Schools. If in any doubt, do not open a suspicious email or attachment and notify the IT Team in accordance with Group Policies. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Online Safety Coordinator and the Group Director of IT.

Further information and advice can be found in the Group's Data Protection, Acceptable Use of IT Policy/Agreement Staff and Governors) and Artificial Intelligence Policies (available on the Group and schools' websites).

20. Breaches of Policy by Staff

Staff should refer to the Group's Staff Code of Conduct Policy which sets out the full expectations for Staff regarding Online Safety and Internet Use, and the Acceptable Use of IT Policy/Agreement (Staff and Governors). The Policy details the repercussions that may follow if these standards are not followed.

A breach of this Policy may be treated as misconduct and as such will be dealt with in accordance with the Group's Disciplinary Policies and Procedures. The Group reserves the right to contact the Police or other outside agency, as appropriate.

Where a member of Staff wishes to complain about Email, internet, social media, electronic images or related electronic communication, or electronic equipment use by another member of Staff, they should inform the Head of the relevant School or if the matter involves a member of the Group Finance, Administration and Support Staff they should inform the Director of Finance and Resources and/or the Director of Operations. A complaint by a member of Staff will be dealt with in a timely and appropriate manner in accordance with the provisions of the Group's Whistleblowing Policy.

If a complaint against a member of Staff is made by a Pupil, Parent/s/Guardian/s/Carer/s concerning a breach of this Policy the matter will be dealt with in accordance with the Group's Concerns and Complaints Policy.

If a breach of this policy raises a safeguarding concern the matter will be dealt with in accordance with the Group's Safeguarding and Protecting the Welfare of Pupils Policy.

21. Visitors' Use of Mobile and Smart Technology

Visitors, including Volunteers and Contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with the Group's Acceptable Use Guidance, and other associated Policies, including Safeguarding Policies. Please note:

- Visitor's Wi-Fi codes are available from the Reception of Group Schools.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or IT Services Manager of any breaches of our Policy.

22. Complaints

As with all issues of safety in Group School's, if a member of Staff, a Pupil, Parent/s/Guardian/s/Carer/s has a complaint or concern relating to online safety, prompt action will be taken to deal with it. Complaints should be addressed to the DSL of the relevant Group School in the first instance, who will undertake an immediate investigation and liaise with the Leadership Team and any members of Staff or Pupils involved. (Please see the Group Complaints Procedure for further information).

23. Review

This Policy shall be reviewed annually by the Court of Governors. and/or following any concerns, and/or updates to national guidance or procedures.

Last Review August 2025
Next Review August 2026

This Policy was approved by the Court of Governors on 17 September 2025 by resolution of the Chair of the Court of Governors, Elliot Lipton.

Signed:

Elliot Lipton
Chair of the Court of Governors

APPENDIX 1: Internet Access and Electronic Safety in Boarding (Mill Hill School, Mill Hill International, Cobham Hall and Heathfield School)

All of the rules and procedures contained within the Group's Online-Safety policy [and Pupil Guidance] apply fully during the formal school day; however, there are a few additions and exceptions which apply within the boarding department after formal school hours.

GENERAL GUIDANCE - All Boarding pupils are subject to the Group's Online Safety Policy at all times when using personal or school electronic devices.

Pupils are forbidden from:

- Downloading music/film which breaches copyright laws
- Accessing gambling sites
- Using unauthorized file-sharing sites
- Using a proxy server with the intention of by-passing the College's 'safe' internet connection
- No pupil may make a recording or take an image of another pupil without their prior consent

Pupils must NEVER use a camera facility in private areas within boarding (e.g. bedrooms or bathrooms).

Pupils accept responsibility for the electronic equipment they bring to school and must ensure it is stored securely (and appropriately insured) If the Online Safety Policy is abused, sanctions may include confiscation of devices, or restrictions on the use of the internet during the evening and the weekend. The Group network is protected by internet safety filters and firewalls. It would be usual that Wi-Fi access is terminated at 11.00pm each night. Some personal electronic devices may allow internet access or the creation of personal 'hotspots'. Pupils may only connect to their own hotspot, which must be password protected. They must not allow others to connect to their hotspot and will be responsible for the safety of their personal password. Pupils remain responsible for their electronic safety when accessing the internet via their own mobile device and must abide by the terms and conditions contained within the Online Safety Policy.

SOCIAL MEDIA ACCESS - All pupils are forbidden from accessing social media sites during the school day; however, for Boarders they can be a key form of communication with family and friends. Social networking sites may be accessed through personal electronic devices but that is conditional on their safe and responsible use.
Pupils must:

- Ensure their privacy settings are set correctly and not to 'open access'
- Only accept friend requests from friends
- Not engage in conversations on-line with people they do not know
- NEVER post inappropriate pictures or contact details about themselves
- NEVER post an inappropriate or defamatory message about another person
- Know how to report or block inappropriate messages on-line
- Report any inappropriate activity on-line to a member of staff

APPENDIX 2: Early Years Online Learning Tools

Tapestry- Online Learning Journal in the EYFS

In Early Years the secure online learning journal Tapestry is used to record observations and make assessments of children's learning. This allows staff and parents to access the information via a personal password protected login. Each child is allocated a class however all staff are able to capture observations for each other's children. Parents logging into the system are only able to see their child(ren)'s learning journal. Parent access allows them to comment (or 'reply') to observations that staff have inputted as well as adding their own observations and photos/videos. Before parents are linked to their child(ren)'s learning journal they are asked to give permission for their child's photo to appear in other children's learning journals. Before beginning to access the system, parents have to sign to agree not to download and share any information on any other online platforms or social networking sites (such as Facebook)

Safe Use Agreement

- Staff and parents should not share log in or password details with any person
- Staff should not share any information or photographs relating to children with any person not employed by The Mill Hill School Foundation.
- Staff should take all responsible steps to ensure the safe keeping of any portable device e.g. iPad that they are using and report any missing devices
- If accessing Tapestry with a private computer, not on Group premises, staff must maintain confidentiality and professionalism
- All entries on Tapestry must be appropriate
- All entries on Tapestry remain the property of the Group
- At all times staff must comply with the Group's Child Protection policies

SeeSaw- Online Learning Journal KS1 (Grimsdell, Keble Prep)

In Y2 each child will have an online portfolio to document their learning. Y2 staff and pupils will have access to their classes portfolios in order to collaborate and support each other's learning. Parents will have access to their own child's portfolio. This will be available through individual personal password protected logins. Teachers, pupils and parents can all give feedback on individual pieces of work; a fantastic way to strengthen home-school links.

Safe Use Agreement

- Staff and pupils should not share log in or password details with any person
- Staff should not share any information or photographs relating to children with any person not employed by The Mill Hill School Foundation
- Staff should take all responsible steps to ensure the safe keeping of any portable device
- e.g. iPad that they are using and report any missing devices
- If accessing SeeSaw with a private computer, not on Group premises, staff must maintain confidentiality and professionalism
- All entries on SeeSaw must be appropriate
- All entries on SeeSaw remain the property of the Group
- At all times staff must comply with the Group Safeguarding and Protecting the Welfare of Pupils Policy, and other related safeguarding policies (see page 3).

Google Classroom is used for Years 1 – 6, and Atom is used for Years 3 – 6 (St Joseph's in The Park)

- The same guidance and Safe Use Agreement as above, also applies to these learning platforms.

APPENDIX 3: Sources of Information for schools and parents to keep children safe online

(from KCSIE, Annex B) (The following list is not exhaustive but should provide a useful starting point).

There is a wealth of information available to support schools and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Advice for governing bodies/proprietors and senior leaders

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- UK Council for Internet Safety have provided advice on, and an Online Safety Audit Tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring
- Department for Digital, Culture, Media & Sport (DCMS) Online safety guidance if you own or manage an online platform provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk.
- Department for Digital, Culture, Media & Sport (DCMS) A business guide for protecting children on your online platform provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

Support for children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Parental support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- How Can I Help My Child? Marie Collins Group – Sexual Abuse Online

- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world.
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Stopitnow resource from The Lucy Faithfull Group can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- Talking to your child about online sexual harassment: A guide for parents – This is the Children's Commissioner's parent guide on talking to your children about online sexual harassment
- #Ask the awkward – Child Exploitation and Online Protection Centre guidance to parents to talk to their children about online relationships
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

Remote education, virtual lessons and live streaming

- Case studies on remote education practice are available for schools to learn from each other
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- Guidance Get help with remote education resources and support for teachers and school leaders on educating pupils and students
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing

APPENDIX 4: Filtering and Monitoring Products in use across Group Schools as of 1 September 2025

No	School	Filtering	Monitoring	Security
1	Mill Hill School	Palo Alto	Senso	ThreatSpike
2	Mill Hill International	Palo Alto	Senso	ThreatSpike
3	Cobham Hall	Palo Alto	Senso	ThreatSpike
4	Heathfield School	Fortinet	Securly	ThreatSpike*
5	Belmont, Mill Hill Prep School	Palo Alto	Senso	ThreatSpike
6	Grimsdell, Mill Hill Prep School	Palo Alto	Senso	ThreatSpike
7	Lyonsdown School	Palo Alto	Senso	ThreatSpike
8	Keble Prep	pfSense	Senso	ThreatSpike
9	Kingshott School	Palo Alto	Securus	ThreatSpike
10	Abbot’s Hill School	Smoothwall	Senso	ThreatSpike*
11	St Joseph’s in The Park	Stormshield	Senso	ThreatSpike
12	Westbrook Hay School	Smoothwall	Securly	Watchguard M370

*** Implementation Phase**

Instilling values, inspiring minds.

Mill Hill
EDUCATION GROUP

The Mill Hill Education Group is the brand name for The Mill Hill School Foundation.
Registered in England: number 3404450
Registered office: Walker House, Millers Close, The Ridgeway, Mill Hill, London NW7 1AQ
Registered charity number: 1064758.