Mill Hill

Primary Academy

INSPIRING CREATIVITY & ACHIEVEMENT

‘Courtesy, Consideration and Respect’

E-SAFETY POLICY

Updated June 2019

Approved:
Review Date:

The e-Safety Policy is an important policy which relates to other policies including those for ICT, bullying and for child protection. The school has appointed an E-Safety Coordinator (D. Watson) and the implementation will be reviewed annually.

The Internet is an essential element in 21st century life for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.

We have a duty to provide pupils with quality Internet access to enhance their learning experiences, which is also safe. Pupils will be taught what Internet use is acceptable and what is not, and they will be given clear objectives for Internet use. They will also be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Curriculum planning will include age appropriate opportunities to discuss, role play and learn about the benefits and risks offered by new technologies, such as mobile phones and social networking sites. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Managing Internet Access

Monitoring Access

- Monitoring software is used to ensure children are safe from threats to their safety, including terrorist and extremist material, when accessing the internet in school.
- Weekly reports are generated and scrutinised by the ICT Leader. Any concerns are investigated using screen grabs from the flagged device. Records of words investigated are kept and any serious incidents are reported to the Headteacher.
- In the event that a child is found to have inputted inappropriate content or visited potentially unsafe sites, the child/children discuss this with the Computing co-ordinator. The Headteacher and parents, if necessary, are informed. Any issues are then logged on CPOMS system (from July 16). Sanctions are run in-line with the school behaviour policy for serious issues.

Word banks containing reference to the following are flagged and reported:
Racism and violence
Suicide and health
Drugs and addiction
Acronyms and general slang
Predators and strangers
Swear words and profanities
Sex words and slang
Pornographic content
Sexual health and biology

- In recording the concerns, a short explanation of context is given to explain the presence of inappropriate content where the child is not responsible for this. This information is then anonymised and data is communicated to the designated School Governor for E-Safety.
- Updates to the monitoring software are completed, where possible, to ensure the most up to date versions are used. Working with the school ICT Technician and the forensic software provider, the ICT Leader will work to establish the most complete coverage of monitoring possible, including with emerging technologies.
- If staff or pupils discover an unsuitable site, the URL must be reported to the school filtering manager (nominated contact) via the ICT Leader.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

SCHOOL WEBSITE

The contact details on the Web site show the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The Head Teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

- Photographs that include pupils will be selected carefully and in line with data permissions and consent procedures.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Permission may be asked for from pupils and parents or carers, before their work will be considered for publication.

Information system security

- Virus protection will be updated regularly on all networked computers.
- School ICT systems capacity and security will be reviewed regularly.
- Filtering requests will be monitored and logged weekly with any teachers being made aware of inappropriate searches involving their class/Key Stage.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication.

Public Web published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- E-mail addresses will be published carefully, to avoid spam harvesting.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Web Publishing pupils’ images and work

- Images published to the web will only include pupils for whom parental permission has been given.
- Pupils’ full names will not be used anywhere on the website, particularly in association with photographs.
- In line with data protection, written permission from parents or carers will be obtained before images of pupils are electronically published to the web.
- Pupils’ work will only be published to the website with the permission of the pupil.

Social networking, Video Messaging and personal publishing

- The City Learning Trust/school will block/filter access to social networking sites, except those specifically purposed to support educationally approved practice.
- Staff and pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Staff and pupils will be advised not to publish specific and detailed private thoughts on social networking sites or blogs (See Section 3).
- Staff and pupils will be advised against video messaging and use of video messaging in school will be banned unless required as part of a specific lesson (e.g.- Speaking to link schools abroad).
- Apps including video and image sharing (eg. Snapchat, Musical.ly, Live.ly) will be included in E-Safety lessons and children will told of the dangers of these.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out and protocols established before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time, unless specifically allowed to support learning as identified by the teacher. The sending of abusive or inappropriate text messages is forbidden. (See Section 4)

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.

Policy Decisions

Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school’s electronic communications, which includes internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil’s access be withdrawn.

- All staff must read this policy before using any school ICT resource.
- At Key Stage 1 access to the Internet will be by directly supervised access to specific, approved on-line materials.

Parents will be asked to read and comply with this policy.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor City Learning Trust can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- E-Safety issues which raise a safeguarding alarm are recorded through the CPOMS system. Details of the incident are included, along with any follow up actions that have taken place. These incidents are to be logged under the following categories: Cyberbullying, Inappropriate Materials, Sexual Behaviour, Stranger Contact, Unsafe Behaviour.
- If a member of staff without access to CPOMs wishes to report a concern, they are to complete the CPOMS report with a member of the Senior Leadership Team.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions will include:
  - interview/counselling by the class teacher;
  - informing parents or carers;
  - removal or restriction of Internet or computer access for a period.

Cyberbullying – Understanding and addressing the issues

While cyberbullying is likely to be low level in primary schools the age of pupils making proficient use of technology is ever decreasing. Therefore, the opportunities for pupils to bully or be bullied via technology, such as e-mail, texts or social networking sites, are becoming more frequent.

As such, teaching pupils about appropriate behaviours when using technology provides a vital grounding for future use. Whilst not wanting to provoke unrecognised opportunities in pupils, consideration must be given to suitable teaching and procedures to address any issues of cyberbullying.

As felt appropriate for the age and use of technology by the pupils:

- The school's anti-bullying policy, E-safety policy and/or school behaviour policy will address cyberbullying. Cyberbullying will also be addressed in Computing, PHSE and other relevant lessons and is brought to life through activities. As with other whole-school policies, all staff and young people will be included and empowered to take part in the process.
- Pupils, parents, staff and governors will all be made aware of the consequences of cyberbullying. Young people and their parents will be made aware of pupils' rights and responsibilities in their use of new technologies, and what the sanctions are for misuse.
- In cases where incidents occur outside of the school environment, the school is committed to investigate and communicate with parents involved. School sanctions can also be used as a result of this behaviour.
- In the event of staff being contacted or referred to in negative or insulting posts online, parents will be required to discuss this with the Headteacher and pupils involved. Advice may also be sought, by the academy, from the Police.

Cyberbullying - How will risks be assessed?

The school will take all reasonable precautions to ensure against cyberbullying whilst pupils are in its care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a school computer will not occur. Neither the school, nor Stoke-on-Trent City Council, can accept liability for inappropriate use, or any consequences resulting outside of school.

The school will proactively engage with all pupils in preventing cyberbullying by:

- understanding and talking about cyberbullying, e.g. inappropriate use of e-mail, text messages;
- keeping existing policies and practices up-to-date with new technologies;
- ensuring easy and comfortable procedures for reporting;
- promoting the positive use of technology;
- evaluating the impact of prevention activities.
- records of any incidents of cyberbullying will be kept and will be used to help to monitor the effectiveness of the school's prevention activities. (Appendix 5)
- the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- methods to identify, assess and minimise risks will be reviewed regularly.

How will cyberbullying reports/issues be handled?

- Complaints of cyberbullying will be dealt with by a senior member of staff.
- The Chair of Govermors to be advised of the fact that there are current issues.
- Any complaint about staff misuse must be referred to the headteacher.
- Evidence of offending messages, pictures or online conversations will be kept, in order to demonstrate to others what is happening. It can be used by the school, internet service provider, mobile phone company, or the police, to investigate the cyberbullying.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions include:
  - interview/counselling by the class teacher;
  - informing parents or carers;
  - removal of Internet/computer access for a period or banning of mobile phone in school.

Communications Policy

Introducing the e-safety policy to pupils

- Pupils will be informed that network and Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- An E-Safety curriculum will be included in Computing programmes covering both school and home use.

Staff and the e-Safety policy

- All staff will be directed to the School E-Safety Policy on the staff shared drive and printed copies will be made available to staff on request. Its application and importance explained.
- All staff will be informed that all computer and Internet use will be monitored. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on the school E-Safety Policy will be provided as required.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy through parents' sessions (when required)
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.

Use of Photography

Introduction

At Mill Hill we welcome positive publicity. Photographs and video clips add colour, life and interest to school activities and initiatives and help the school community to identify and celebrate the school's achievements. We recognise that images must be used in a responsible way, respect young people's and adults' rights of privacy and are aware of child protection issues. However, we need to balance the risk against promotion. Risks can be minimised by following the guidelines detailed in this policy.

Data Protection Act

Photos and video images of pupils and staff are classed as personal data under the terms of the General Data Protection Regulations. For this reason, we require the consent of either the individual concerned or in the case of pupils under the age of 13, their legal guardians before we can display these images in the media, in publications, on websites or in public places.

Child Protection Issues

Risk occurs when individual pupils can be identified by their names alongside photographs. Therefore, we will give the first name of the children in photographs that are displayed within the school building. We will not provide names for any other purpose unless special parental consent has been received. Only images of children in suitable dress will be taken. Should the school learn about any inappropriateness of image use involving our pupils, we will immediately act and report it as we would for any other child protection issue.

Images taken by school staff

- Staff should not use recording equipment on their mobile phones, for example: to take recordings of children. If, however, a significant learning opportunity would be otherwise missed, staff may use them with discretion. Recordings must be downloaded to secure networks and then removed from the personal device at the soonest opportunity.
- Legitimate recordings and photographs should be captured using school devices: cameras and iPads.
- Staff should report any usage of mobile devices that causes them concern to the Headteacher.

Images taken by adults other than school staff

The school regularly reminds parents that images of children (other than their own) should not be posted online on social media etc. When a commercial photographer/film maker (e.g. Academy) is used we will:

- Provide a clear brief

- Issue identification
- Inform parents and children
- Obtain consent
- Not allow unsupervised access to children

Social Media

Objectives

This policy sets out Mill Hill Academy's policy on social networking. Social networking activities conducted online outside work, such as blogging, involvement in social networking sites such as Facebook or Twitter and posting material, images or comments on sites such as You Tube can have a negative effect on an organisation's reputation or image. This policy has been written to set out the key principles and code of conduct that we expect of all members of staff with respect to their responsibilities in connection with the use of social networking sites.

Key Principles

- Everyone at Mill Hill has a responsibility to ensure that they protect the reputation of the school, and to treat colleagues and members of the school with professionalism and respect.
- It is important to protect everyone at Mill Hill from allegations and misinterpretations which can arise from the use of social networking sites.
- Safeguarding children is a key responsibility of all members of staff and it is essential that everyone considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer must not communicate with children via social networking.
- This policy relates to social networking outside work.

Code of Conduct: Social Networking

Under no circumstances should staff make negative reference to any staff member, pupil, parent or school activity/event.
The following are also **not considered acceptable**:

- The use of the school's name, logo, or any other published material without prior permission from the Headteacher. This applies to any published material including the internet or written documentation.
- The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.
- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.
- The posting of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.

In addition to the above everyone must ensure that they:

- Never ‘friend’ a pupil at the school where they are working onto their social networking site.
- Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.
- Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor the school’s reputation is compromised by inappropriate postings.

Potential and Actual Breaches of the Code of Conduct

In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Use of social media will be monitored annually and any breaches of this code will be investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure. A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school’s ethos and principles.
- The Governing Body will take appropriate action in order to protect the school’s reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.

Mill Hill Facebook Page

- The Mill Hill Facebook page is visible to all those who join the group. This means that any parents, carers or others may be able to view personal pages. Be sure to keep personal pages suitable for such viewing.
- The ICT lead (D. Watson) has sole control of publishing material on the page. He monitors all activity on the page and informs he Headteacher of any material posted, which infringes the agreed policy with parents / carers.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document.

Mobile Devices

Introduction and Aims

At Mill Hill the welfare and well-being of our pupils is paramount. The aim of the Mobile Phone Policy is to allow users to benefit from modern communication technologies, whilst promoting safe and appropriate practice through establishing clear and robust acceptable mobile user guidelines. This is achieved through balancing protection against potential misuse with the recognition that mobile phones are effective communication tools.

Personal Mobiles - Staff

- Staff are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office so that cover can be provided. This includes serious messages e.g. news of an unwell family member. It is not appropriate to take a serious call when pupils are present as they may be left in a vulnerable situation if a member of staff becomes distressed. If a member staff considers their circumstance warrants use of phone this must be agreed with the Headteacher.
- Staff should have their phones on silent or switched off and out of sight (e.g. in a drawer, handbag or pocket) during class time.
- Mobile phones should not be used in a space where children are present (e.g. classroom, playground).
- Use of phones (inc. receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms.
- It is also advised that staff use security measures to protect access to functions of their phone.
- Staff should not use recording equipment on their mobile phones, for example: to take recordings of children. If, however, a significant learning opportunity would be otherwise missed, staff may use them with discretion. Recordings must be downloaded to secure networks and then removed from the personal device at the soonest opportunity.
- Legitimate recordings and photographs should be captured using school devices: cameras and iPads.
- Staff should report any usage of mobile devices that causes them concern to the Headteacher.

Mobile Phones for work related purposes

We recognise that mobile phones provide a useful means of communication on offsite activities. However, staff should ensure that:

- Mobile use on these occasions is appropriate and professional.
- Mobile phones should not be used to make contact with parents during school trips. Where possible, all communications should be made via the school office/ Facebook (via D. Watson). If the trip take place outside office hours, it may be necessary to use personal phones in some circumstances.
- Where parents are accompanying trips, they are informed not to make contact with other parents (via calls, text, email or social networking) during the trip or use their phone to take photographs of children.

Other Devices

Through the course of teaching, staff will require some pieces of equipment to be removed from the premises. Laptops, iPads and other items can be taken home but staff should ensure that:

- Items are password protected

- Best security measures are in place (storage in car boots, not left visible in homes etc.) to reduce the chance of theft or damage.
- Devices should only be used for school related business. The use of devices for other means opens the possibility of security issues or viruses.

Personal Mobiles – Pupils

We recognise that mobile phones are part of everyday life for many children and that they can play an important role in helping pupils to feel safe and secure. However, we also recognise that they can prove a distraction in school and can provide a means of bullying or intimidating others. Therefore:

- A Home/School Agreement Mobile phone form must be completed and signed.
- The phone must be handed in, switched off, to the school office first thing in the morning and collected from them by the child at home time (the phone is left at the owner’s own risk).
- Mobile phones brought to school without permission will be confiscated and returned at the end of the day.
- Where mobile phones are used in or out of school to bully or intimidate others, the then the head teacher does have the power to intervene ‘to such an extent as it is reasonable to regulate the behaviour of pupils when they are off the school site.

Volunteers, Visitors, Governors and Contractors

All Volunteers, Visitors, Governors and Contractors are expected to follow our mobile phone policy as it relates to adults whilst on the premises. On arrival, such visitors will be informed of our expectations around the use of mobile phones.

Parents

While we would prefer parents not to use their mobile phones while at school, we recognise that this would be impossible to regulate and that many parents see their phones as essential means of communication at all times. We therefore ask that parents’ usage of mobile phones, whilst on the school site is *courteous* and *appropriate* to the school environment and is in keeping with this policy.