Mill Lane Community School &
The Windmill Community Nursery

Growing, Thriving, Flying

E-Safety Policy

This policy applies to Mill Lane Community Primary School and the attached Windmill Community Nursery as well as the extended services provision provided by Mill Lane.

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students / pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and safeguarding policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, whilst also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development, Monitoring and Review

This e-safety policy was approved by the governing body in January 2022 and the implementation of this e-safety policy will be monitored by the Behaviour and Well-Being Committee. Monitoring will take place every 2 years. The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of pupils, parents / carers and staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors and community users.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the governors and the governors on the Behaviour and Well-Being Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of ICT & E-Safety Governor. The role of the ICT & E-Safety Governor will include:

- regular meetings with the ICT Co-ordinator
- regular monitoring of e-safety incident logs
- reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the ICT coordinator
- The Headteacher is responsible for ensuring that the ICT Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Senior Leadership Team will receive regular monitoring reports from the ICT coordinator
- The Headteacher and Deputy Head should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

ICT Coordinator

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school's e-safety policy and documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff
- Liaises with the School ICT technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets with the e-safety governor to discuss current issues and review incident logs
- Attends relevant meetings

School's Network Provider

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the e-safety technical requirements
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- They keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

Teaching and Support Staff

- They have an up to date awareness of e-safety matters and of the current e-safety policy and procedures
- They have read, understood and signed the school 'Staff Acceptable Use Policy'
- They report any suspected misuse or problem to the ICT coordinator or Headteacher for investigation
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils follow the school e-safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use

Designated Person for Child Protection

The designated person should be trained in e-safety issues and be aware of the potential for child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils

- Are responsible for using the school ICT system in accordance with the 'Pupil Acceptable Use Policy' which they will be expected to sign before being given access to school systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every available opportunity to help parents understand these issues through parents' evenings, newsletter, and website. Parents / carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy

Teaching and Learning

The internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality internet access as part of their learning experience:

- The school internet access will be designed expressly for pupil use including appropriate content filtering
- Pupils will be given clear objectives for internet use and taught what use is acceptable and what is not
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- As part of the new Computing (ICT) curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, our digital footprint and cyber-bullying and are part of the 'PurpleMash' computing scheme of work
- When children are directed to websites as part of home learning, they will have been checked for appropriateness by the teacher setting the learning.

World Wide Web

The internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL, time and content shall be reported to the teacher who will then record the incident in the e-safety log which will be stored in the ICT suite. The e-safety log will be reviewed termly by the ICT coordinator.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy
- The school will work with its technical support providers to ensure filtering systems are as effective as possible

Email

Email is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:

- Pupils may only use approved email accounts on the school system
- Pupils must immediately tell a teacher if they receive offensive email
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission
- Whole class or group email addresses should be used in school rather than individual addresses
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding

Social Networking

Social networking internet sites provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face to face contact.

- Use of social networking sites in school is not allowed and will be blocked / filtered
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils
- Pupils will be encouraged to only interact with known friends and family over the internet and deny access to others
- All staff are advised not to have contact with parents and children on any social networking site
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber-bullying and defamatory comments.

Mobile Phones

Many new phones have access to the internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety / precautionary use. These are handed to the class teacher/ when the child arrives and collected at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom or on the playground.
- Parents cannot use mobile phones on school trips to take pictures

Digital / Video Cameras

Pictures, videos and sound are not directly connected to the internet, but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff
- Parents will not use digital cameras, mobile phones or video equipment at school unless specifically authorised by staff
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on the school website, particularly in association with images
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website
- The headteacher or nominee will inform parents / carers and others present at school events that photographs / videos may be taken on the basis that they are for private retention and not for publication in any manner

School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the website will be the school address, email, telephone and fax number.
- Staff and pupils' personal information will not be published
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs
- Consent from parents will be obtained before photographs of pupils are published on the school web site
- Parents may upload pictures of their own child on to social networking sites. If the picture includes another child / children then it is their responsibility to gain permission from that child's parents.
- The governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly
- E-safety will be discussed with our ICT support and those arrangements incorporated in our agreement with them.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by the headteacher
- Any complaint about staff misuse must be referred to the headteacher
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures

- Pupils and parents will be informed of the complaints procedure
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues

Communication of Policy

Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed when they are in KS2 of the importance of being safe on social networking sites such as msn. This will be strongly reinforced across all year groups during ICT lessons and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

- All staff will be given the School e-safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

Parents:

- Parents' attention will be drawn to the School e-safety Policy in newsletters and on the school Website.

Reviewed & updated: January 2024

Next Review: January 2027

Signed on behalf of the Full Governing Body:

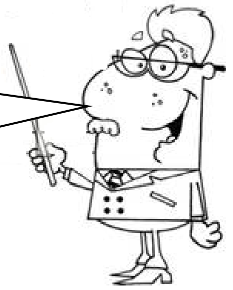
Appendix 1

Guidelines to Accidental Inappropriate Internet Access

What should you do if a child **accidentally** finds a website displaying inappropriate material? Follow these step by step instructions:

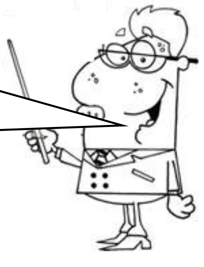
1. Praise the pupil for reporting the incident.

2. Explain to the pupil that, in order to prevent it happening again, you need to ascertain how the pupil gained access to the inappropriate material.



3. Ask the pupil to explain what happened.

4. Ask a designated member of staff to phone the School Service Desk with the details of the incident so that the OCN filtering can be improved accordingly.

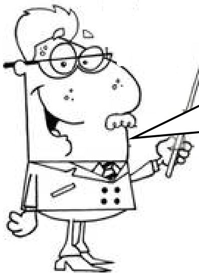


Report the incident to the headteacher. If appropriate inform the pupil's parents to explain the preventative action that will be taken by the school.

Appendix 2

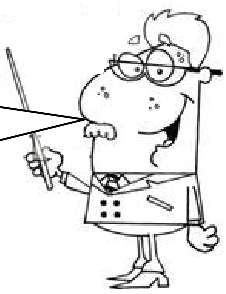
Guidelines to Deliberate Inappropriate Internet Access

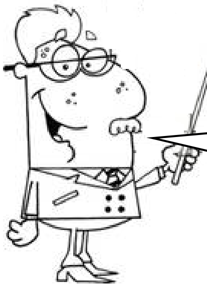
What should you do if you find a child **deliberately** searching for inappropriate materials on the internet? Follow these step by step instructions:



1. Explain to the pupil that they have broken the rules of your school's Acceptable User Policy (AUP) and Internet Code of Conduct, and that their behaviour is unacceptable.

2. Take the pupil off the computer for the rest of the lesson. Ask the pupil to explain what happened and tell them that by doing so they may lessen the seriousness of the incident.





3. Remind children of the Internet Code of Conduct they signed when they started school and which is displayed on a poster in the ICT suite.

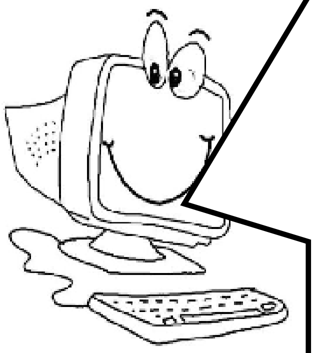
4. Discuss the incident with the ICT coordinator and ensure it is reported to the school's service desk by a designated member of staff so that OCN filtering can be improved accordingly.

Report the incident to the headteacher. Remove the child from the computer for the rest of the lesson, during which time the child should take time to reflect on and write down what they did wrong. A letter should go home to parents of the child directly involved in the incident. A letter to all parents of children in the class must be sent home explaining what has happened.

Mill Lane School
ICT Code of Conduct
Be Responsible Stay Safe on Computers

Appendix 3

These rules for sensible Internet and ICT use will ensure our safety. Please make sure you understand and keep to them.
Use of computers is for educational purposes.



1. Only use the internet when there is a teacher or other adult present to supervise, or when you have permission
2. Only use your own login and password.
3. Never give out your address, phone number or arrange to meet someone.
4. All e-mails should be polite, appropriate and sensible.
5. If you receive a rude or offensive message you must report it to a member of staff immediately.
6. If you see anything offensive or if you feel uncomfortable about anything, report it.
7. Be aware that the school may check your computer files and monitor the Internet sites you visit.
8. Make sure that a web source is reliable and information you are going to use is accurate.

I understand that if I break any of these rules I will be moved off the computer and my parents will be informed.

Be Sensible and Be Safe

Appendix 4

INTERNET
PERMISSION FORM

Pupil

Name:…………………………………………Class………..Date…………..………

My Parents and I have read the code of Conduct for internet use and I agree to follow it.

Signature…………………………………………………

Parent

As Parent/Guardian I have read, discussed and explained the code of Conduct to my son/daughter. I understand that if he/she fails to follow the Code of Conduct for Internet Use, access will be withdrawn and I shall be informed.

I grant permission for…………………………………………to access the internet.

Parent/Guardian signature………………………………………………….

Copyright Release

This school may produce web pages, ICT presentations, educational or interest articles for magazines or similar. No child's work will ever be used without his/her permission, but we also need permission from the parents to be able to publish the child's work. Please rest assured the child's safety will always be of paramount importance, no personal information will be made public.

Please sign this copyright release if you are happy for your child's work to be shared in this way. (This arrangement can be changed at any time by contacting the school office.)

I consent for the school to publish my child's work on the internet subject to strict confidentiality of personal information.

Parents/Guardians signature………………………………………………

Privileges – The use of the internet is a privilege not a right, inappropriate use will result in a cancellation of those privileges.

Mill Lane Community Primary School
Internet form