e-Safety Policy

We believe that the use of information and communication technologies in schools brings great benefits. Recognising the e-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications. This Policy will help inform parent about e-Safety.

e-Safety Disclaimer

We have made every effort to ensure that the information in this document is accurate and up to date. If errors are brought to our attention, we will correct them as soon as practicable.

Nevertheless, Meadow Hall School and its employees cannot accept responsibility for any loss, damage or inconvenience caused as a result of reliance on any content in this publication.

1. Why we need an e-Safety Policy

In today's society, children, young people and adults interact with technologies such as mobile phones, game consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

e-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communication technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff and parents need to be aware of the importance of good e-Safety practice in the classrooms and at home in order to educate and protect our children.

Breaches of an e-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that we are all aware of the offline consequences that online actions can have.

This policy provides a range of statements to make policy viewing easier and more comprehensive. For simplicity we have used the terms 'school', 'pupils' and 'students' in the document.

2. Who will review the policy?

The head teachers and board of governors have a responsibility to safeguard children and staff and this includes online activity.
The school has appointed an e-Safety Coordinator, Mr Ayodeji Aremu (ICT Manager).

The School's Designated Child Protection Coordinator (DCPC) will need to be aware of an e-Safety training and resources will be available should any child wish to disclose information regarding an online incident.

The School's DCPC is the head of each section; Mrs Oluyemi, Miss Ekpenyong and Mrs Adepoju

The e-Safety Policy and its implementation will be reviewed annually.

The date for the next policy review is May 2015.

3. How to use this document.

It is recommended that parents see e-Safety as a whole school issue. As such, they should develop a holistic approach to supporting and implementing the school's e-Safety Policy as well as embedding safe practice.

It is strongly recommended that all stakeholders (staff, parents/carers, pupils etc.) should be actively involved in implementing this e-Safety policy to collaboratively create a safer e-learning experience for our children.

Teaching and learning

4. Why is Internet use important?

Rationale:
The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through ICT and Internet use.

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

5. How does Internet use benefit education?

Rationale:
A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:
- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with other schools worldwide.
- Access to learning wherever and whenever convenient: e-delivery and e-assessment.

6. How can Internet use enhance learning?

Rationale:

Increased computer numbers and improved Internet access may be provided but its impact on pupils learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Methods to detect plagiarism may need to be developed.

- The school's Internet access will be designed to enhance and extend education.
- Pupils shall be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff shall guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will 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 acknowledge the source of information used and to respect copyright when using Internet material in their own work.

7. How will pupils learn how to evaluate Internet content?

Rationale:

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc provide an opportunity for pupils to develop skills in evaluating Internet content. For example researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

The following statements require adaptation according to the pupils' age:
- Pupils shall be taught to be critically aware of the materials they read and will be shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

8. How will email be managed?

Rationale:
Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits, for example, interesting projects between schools in neighbouring villages and in different continents can be created.

The implications of email use for the school and pupils need to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to pupils that bypass the traditional school boundaries.

Spam (unsolicited emails), phishing and virus attachments can make emails dangerous, which could lead to loss of money, scams, identity theft, loss of valuable data, malware (malicious software) and a lot of other problems. For the above reasons:

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell their ICT or class 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 from an adult.
- Whole class or group email addresses will be used in primary schools for communication outside of the school.
- Staff will only use official email accounts provided by the school to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Social email use can interfere with learning and will be restricted.
- The forwarding of chain messages is not permitted.

9. How will social networking, social media and personal publishing be managed?

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

For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

- The school will control access to social media and social networking sites.
- Pupils should never give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc..
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Accessing auction sites such as eBay, Amazon etc is prohibited.

10. How will filtering be managed?

Rationale:
Levels of Internet access and supervision will vary according to the pupil's age and experience. Access profiles must be appropriate for all members of the school community. Older secondary pupils, as part of a supervised project, might need to access specific adult materials; for instance a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use would be recognised and restrictions removed temporarily. However if access to such material is being used in school, teachers would monitor closely, likewise parents would be notified if need be. However, systems to adapt the access profile to the pupil's age and maturity are available.

Access controls fall into several overlapping types (commonly described as filtering):
- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- A ''walled garden'' or "allow list" restricts access to a list of approved sites. Such lists inevitably limit pupils' access to a narrow range of content.
- Dynamic content filtering examines web page content or email for unsuitable words.
- Keyword lists filter search engine searches and URLs for inappropriate results and web addresses. Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject rated pages exceeding a threshold.
- URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate pupil access.
- Key loggers record all text sent by a workstation and analyse it for patterns.

It is important that parents recognise that filtering is not 100% effective. There are ways to bypass filters, however we will endeavour to keep abreast of filtering circumvention.

Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children should always be supervised when using the Internet at

home. In addition, Internet Safety rules should be displayed, and both children and adults should be educated about the risks online.

- The School's broadband access will include filtering appropriate to the age and maturity of pupils.
- If staff or pupils discover unsuitable sites or sites they deem inappropriate, they should immediately speak to an ICT teacher if in school, or a responsible adult if at home.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.

11. How are emerging technologies managed?

Rationale:
Many emerging communication technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment will be undertaken on each new technology for safe and effective incorporation into classroom practice.

Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within school systems. Online communities can also be one way of encouraging a disaffected pupil to keep in touch.

The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites and other online tools such as Facebook, YouTube, Skype and Twitter. However, staff and parents should insist that students strictly observe age restrictions on such sites.

12. How will Internet access be authorised?

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

Parents will be asked to read the e-Safety Policy for pupil access and discuss it with their child, where appropriate.

All visitors to the school site who require access to the school's network or internet access will be asked to read and sign an Acceptable ICT Use Policy. Pupils will only be provided with supervised Internet access appropriate to their age and ability.

When considering access for vulnerable members of the school community (such as with children with Special Education Needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

13. How will risks be assessed?

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Hence, the school will not be held liable for the material accessed, or the consequences thereof.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- Students are not to bring into the school environment, games, screen savers, mobile devices such as iPhones, Ipads, iPods, Cell phones, Tablets (except provided by the school) etc without written consent from the school for specific projects.

14. How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The ICT manager will record all reported incidents and actions taken in the School e-Safety incident log, as well as update other records, such as Bullying or Child Protection log.
- The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents or concerns as and when required.
- Following a concluded investigation, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Police

15. How will e-Safety complaints be handled?

Complaints about Internet misuse will be dealt with under the School's complaints procedure.
Any complaint about staff misuse will be referred to the Head Teacher.
All e-Safety complaints and incidents will be recorded by the school, including any actions taken.
Pupils and parents will be informed of the complaints procedure.
Parents and pupils will need to work in partnership with the school to resolve issues.
All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
All members of the school community are reminded to only engage in safe and appropriate behaviour online. Also, kindly remember not to post any content, comments, images or videos online which may cause harm, distress or offence to any other members of the school community.

16. How will Cyberbullying be managed?

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's anti-bullying and behaviour policy.

All incidents of cyberbullying reported to the school will be recorded.

There are clear procedures in place to investigate incidents or allegations of Cyberbullying.
● The school will keep a record of the bullying as evidence.
● The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
● Pupils, staff and parents/carers will be required to work with the School to support the approach to cyberbullying and the school's e-Safety ethos.
● Sanctions for those involved in cyberbullying may include:
    ▪ The bully is asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    ▪ Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable ICT Use Policy.
    ▪ Parent/carers of pupils will be informed.
    ▪ The police will be contacted if a criminal offence is suspected.

17. How can parents' support be enlisted?

● A partnership approach to e-Safety at home and at school with parents is encouraged.
● Parents will be requested to sign an e-Safety /Internet agreement as part of the Home School Agreement, at the start of term
● Parents will be encouraged to read the School's Acceptable ICT Use Policy for pupils and discuss its implications with their children.
● Information and guidance for parents on e-Safety will be made available to parents in a variety of formats.
● Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.