Moorside
Primary School

E-safety Policy – Moorside Primary School

Responsibility

Senior leads with responsibility for whole school computing, online safety and Safeguarding responsibility: Head Teacher: Mrs L. Hall, Deputy Head Teachers: Miss S. Rowe and Miss N Harris.
Computing Lead: Mr C Watson
Technician LA/ICT Services: Mr K Gibson

The monitoring of e-safety is the responsibility of the Head Teacher, Senior Leadership Team, and the Computing lead.

As online safety is an important aspect of strategic leadership within the school, the Head Teacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the Computing lead and senior leaders to keep abreast of current issues and guidance through organisations such as Newcastle Local Authority, Department for Education, Child Exploitation and Online Protection Centre (CEOP), and Childnet.

Senior Leadership, Governors and computing lead have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice. This policy, supported by the school's acceptable use agreement for staff and Code of Conduct for pupils, is to protect the interests and safety of the whole school community.

It is linked to the following mandatory school policies:

- Keeping Children Safe in Education
- Child Protection
- Health and Safety
- Behaviour (including the Anti-Bullying)
- Acceptable Use
- PSHCE (Personal, Social, Health and Citizenship Education).

Introduction

Computing and the use of digital devices are an essential resource to support teaching and learning, as well as playing an important role in the everyday lives of children, young people and adults. As a school, we aim to build in the use of these technologies in order to provide pupils with the skills to access life-long learning and employment.

Computing and ICT (information and communications technology) covers a wide range of resources including web-based and mobile learning. It is important to recognise the constant and fast paced evolution of computing within our society as a whole. Currently the Apps and software children and young people are using both inside and outside of the classroom include:

- Websites for researching
- Coding
- Gaming
- Mobile devices
- Video & Multimedia
- Audio

Whilst exciting and beneficial all users need to be aware of the range of risks associated with the use of these technologies. At Moorside Primary School we understand the necessity to educate pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies. The content is differentiated and age appropriate, showing the progression of this knowledge throughout school.

Moorside
Primary School

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head Teacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Computing lead at Moorside Primary School is Mr C Watson.

Key Tasks of the Computing lead

- Develop an e-safe culture throughout the setting as part of safeguarding that is in line with national best practice recommendations.
- Act as a named point of contact on e-safety issues and liaising with other members of staff as appropriate.
- Audit and evaluate current practice to identify strengths and areas for improvement. This is carried out using the Kent Self-evaluation tool and 360 safe.
- Keep up to date with current research, legislation and trends. This may include accessing appropriate training and using a range of approaches to enable them to understand the role of new technology as part of modern British society and the wider safeguarding agenda.
- Embed e-safety through staff training and CPD by ensuring that all members of staff receive up to-date and appropriate e-safety training (at least annually and as part of induction) which sets out clear boundaries for safe and professional online conduct.
- Ensure that there is an age and ability appropriate e-safety curriculum that is embedded, progressive, flexible and relevant which engages children's' interest and promotes their ability to use technology responsibly and to keep themselves and others safe online.
- Ensure that the setting participates in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensure that e-safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Ensure that age-appropriate filtering is in place, which is actively monitored
- Ensure all e-safety concerns are reported to senior leadership and through the use of CPOMS (Safeguarding and Child Protection Software for Schools).
- Liaise with the local authority and other local and national bodies as appropriate.
- Review and update e-safety policy on a regular basis (at least annually) to ensure that e-safety is integrated with other appropriate school policies and procedures.
- Monitor and report on e-safety issues to the school management team, CPOMs, Governing Body and other agencies as appropriate.

E-safety in the Curriculum

As a school we provide opportunities within a range of curriculum areas to teach about e-safety. Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-safety curriculum, including during our after school clubs.

The teaching of e-safety focuses on helping pupils to recognise inappropriate content, conduct, contact and commercialism and helps them learn how to respond or react appropriately. Pupils need to be aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils should know how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or through an organisation such as Childline and CEOP (Child Exploitation and Online Protection Command) used for reporting abuse. As a school, each year, we participate in e-safety activities during 'Safer Internet Day' to continually re-enforce the messages.

Managing the Internet

All internet activity within school is monitored and filtered through Newcastle LA Civic Centre's Smoothwall system. Whenever any inappropriate use is detected, the school is notified and the incident will be followed up in line with the school Acceptable Use Policy.

The school maintains pupils will have supervised access to internet resources through the school's digital devices. We aim to limit the reliance of the internet for homework however when children want

to use it to support their work we re-enforce our e-safety messages and encourage appropriate parental supervision.

Infrastructure
Our internet access is provided by Telewest Broadband and monitored by Smoothwall. Curriculum access is managed by the Computing lead alongside the senior leadership team. Staff and pupils need to be aware that should they encounter or access anything unsuitable or damaging they must report it immediately to teachers who will then follow appropriate safeguarding procedures.

Mobile Technologies Personal Mobile devices (including phones)
The school allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom. These are not to be used at any time whilst in the presence of pupils. Mobile phones are not permitted in the learning areas during the school day while pupils are present. Personal mobiles are not permitted on school visits school mobiles are used for such events. Within working hours, staff must have proper and professional regard for the policies and practices of the school in which they teach which are linked to the use of mobile technologies.

Visitors intending to work with pupils are requested to keep their mobile phone in a safe locker during the day with access available when not working with pupils. Any personal mobile devices do not have access to the internet via the schools WiFi network. The school is not responsible for the loss, damage or theft of any personal mobile device.

Managing emails
The use of emails within school is an essential means of communication for staff. Pupils do not access individual email accounts within school. Staff must use the school's approved email system for any school business. Staff must inform the school safeguard lead (Head Teacher) if they receive an offensive or inappropriate e-mail.

Social Networking
The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day. The Smoothwall monitoring filters out the access to all social media platforms. We also strongly discourage children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which have a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take appropriate actions. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

Safe Use of Images
Creation of videos and photographs
With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. All staff are aware of specific children (they have responsibility for) in school which do or do not have photograph permissions. If they do have permission, staff are aware of which platforms they can be used on.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes field trips. School's own mobile devices must be used in this case.

Publishing pupil's images and work
All parents/guardians will be asked for their permission for their child's work/photos in publicity materials or on the school website or other online presences. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. Parents/ carers may withdraw or amend permission, in writing, at any time.

Pupils' full names will not be published alongside their image and vice versa on the school website or any other school based publicity materials.

Moorside
Primary School

Storage of Images
Images/ films of children are stored securely on the school server, not on individual iPads and / or teacher's individual school laptops, and not personal laptops.

Complaints
Complaints or concerns relating to e-safety should be made to the Safeguarding lead (Head Teacher), and senior leadership team.

Inappropriate material
All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the safeguard lead (Head teacher). Deliberate access to inappropriate materials by any user will lead to the incident being logged, in the first instance, by Smoothwall and then forwarded to the school and in turn, the safeguard lead (Head teacher).. Depending on the seriousness of the offence; investigation maybe carried out by the Head teacher or LA. Staff should be are aware that negligent use or deliberate misconduct could lead to disciplinary action.

Equal Opportunities
The school endeavours to deliver a consistent message to parents and pupils with regard to the schools' e-safety rules. Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues. Internet activities are planned and well-managed for these children and young people.

School Website
Our school website promotes and provides up to date information about the school. In order to minimise risks of any images of pupils on the school website being used inappropriately the following steps are taken;

- Pupils are not named on any image that is used on the website.
- The website does not include any home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff.

Points for Parents to consider

- Take an interest in what children are doing.
- Discuss with the children what they see and why they are using the internet.
- Monitor on-line time and be aware of excessive hours spent on the internet.
- Discuss that there are websites that are unsuitable.
- Discuss how children can respond to unsuitable material/requests.
- Inform children to never give personal information on the internet.
- Remind children that people on-line may not be who they say they are.
- Be vigilant – ensure that children do not arrange to meet someone they meet on-line.
- Be aware that children may be using the internet in other places than their own home or at school.

Points for children to consider

- Always keep your name, address, mobile phone number and passwords private.
- Never arrange to meet with someone you have had contact with over the Internet.
- Do not accept emails or open files from people you do not know or trust as they may contain viruses or nasty messages.
- Remember someone on-line may not be who they say they are.
- Tell your Parent/Carer if someone or something makes you feel uncomfortable or worried.

For further information, please see the following:
http://www.bbc.co.uk/cbeebies/grownups/article-internet-use-and-safety
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/