Moston Lane Community Primary School

E Safety and Computing Policy

Headteacher: Mrs Judy Kerton

Moston Lane Community Primary School, Moston Lane, Manchester M9 4HH
Tel: 0161 205 3864 - Fax: 0161 205 7721
Email: admin@mostonlane.manchester.sch.uk

COMPUTING POLICY

At Moston Lane Primary School we seek to develop children's understanding and appreciation of ICT and the way it impacts on our lives. We believe it is essential to provide opportunities in all National Curriculum subject areas for children to develop their ICT capability and to use it to support their learning. ICT makes education accessible to all, irrespective of learning styles and individual needs. At Moston Lane ICT education is provided in a safe, happy and disciplined environment to stimulate and challenge both pupils and staff.

Aims & Objectives

- ✓ To encourage children to develop positive attitudes to ICT and to understand its importance and relevance to today's world.
- ✓ To enable children to acquire a broad range of ICT capabilities and to be confident about using a range of hardware and software.
- ✓ To enable children to develop ICT as a tool for learning and investigation in all subject areas.
- ✓ To use ICT to encourage children to work co-operatively, taking responsibility collectively.
- ✓ To use ICT to develop independent ways of working which encourage children to take responsibility for their own actions.
- ✓ To set ICT tasks which require flexibility of mind and open mindedness in problem solving.
- ✓ To provide a balanced range of progressively more difficult tasks which will develop children's understanding in *Communicating and handling information, Controlling, Modeling and Monitoring.*
- ✓ To instruct children in the use of a variety of ICT equipment.
- ✓ To ensure a balance of ICT activities are carried out in a range of contexts.
- ✓ To provide opportunities for children to explore the use of Technology.
- ✓ To set aside time for discussion of children's experience of using ICT, both in and out of the classroom.
- ✓ Computing to enhance whole curriculum.

Teaching & Learning
Teaching and learning in the computer suite will be based with an emphasis on whole class activities. New knowledge or skills will be taught by the teacher to the class and these will be reinforced by the class activities using the computers. There will be lessons where the teacher is repeating a skill in order for the children to understand it or to further their knowledge.

Planning
The curriculum map and scheme of work sets out the knowledge, skills and understanding to be taught, along with suggested activities. This will ensure coverage of the National Curriculum, progression of skills, knowledge and understanding, and the use of ICT in all subject areas.

Staff use schemes of work and medium term planning to produce weekly plans.
The curriculum coordinator over sees these plans.

Differentiation by task, support or outcome will be used to support and extend all children. Short focused tasks will be used for children to consolidate or enrich skills learned.

Each subject coordinator will also incorporate ICT activities in his/her own scheme of work and is jointly responsible, with the ICT coordinator, for their implementation and monitoring.

Foundation Stage
The early learning goals are the key focus for ICT and these are incorporated in the long, medium and short term plans.

SEN
For children with SEN, ICT can provide a means of reinforcing concepts and knowledge. ICT has excellent motivational potential for children experiencing learning difficulties or behavioural problems, for example using a word processing program supports presentational skills and a spell check may help with spellings. To fully consolidate their skills, SEN children may require greater access to ICT in short, frequent sessions.

Equal Opportunities
Each child regardless of gender, ability, social and cultural background has an equal entitlement to ICT capability. Activities may be adapted to ensure a full programme of ICT is provided for children with physical disability or impairment.

Assessment & Recording
Assessments are used to inform the planning for consolidation and development of ICT capability. Teachers will assess pupil's progress against the National Curriculum and the Clive Davis scheme of work.

During a topic, the work completed will be stored on the main server and is accessible by all staff.

All children to have a computing portfolio that will have 1 piece of work (photo, screen grab) per half term recorded.

Resources
Each classroom has at least one networked computer. The ICT suite has 32 networked computers and an interactive whiteboard. Each Year Group has access to a wide range of software as well as the Internet.

There are also networked computers in the PPA room and learning bases. Each class has an interactive whiteboard, which are used daily to enhance teaching and learning. The school has a class set of IPads. All other hardware and software can be found on the server or distributed to the appropriate year groups. In addition to the computers there is a range of other ICT resources including a digital camera for each class, digital viewer, sound recorders, mini video recorders, control devices (e.g. Beebots) and digital microscopes. The hall computers are networked and connected to a projector and sound system.

Year 6/5 have apple technology in the classroom that can be shared by all staff in upper key stage 2 when required.

The school currently has 26 operational iPads that are available to any teacher.

Each staff member has a staff iPad that has extra fewer restrictions on them such as access to YouTube.

Monitoring & Review
The ICT coordinator is in charge of planning, monitoring and evaluating the use of ICT in school, providing support, organising training and arranging whole school INSET when appropriate and in conjunction with LA initiatives.

The ICT coordinator and the school technician are responsible for monitoring the condition of ICT equipment in school and organizing repair/ replacements as and when it is necessary. The computing coordinator should plan ahead to ensure the continuous updating of equipment and resources.

The ICT coordinator is responsible for reviewing and updating the ICT policy and the schemes of work. The coordinator should carry out a subject scrutiny and observe teaching and learning. Whenever a curriculum is reviewed, as part of staff or curriculum development, the use of ICT in that particular subject will be an integral part of the training/planning.

The Acceptable Use of the Internet and related Technologies

Whole school approach to the safe use of ICT
Creating a safe ICT learning environment includes three main elements at this school:

- ✓ An effective range of technological tools;
- ✓ Policies and procedures, with clear roles and responsibilities;
- ✓ A comprehensive e-Safety education programme for pupils, staff and parents.
- ✓ Safe search engines. E.g www.safesearch.com www.primaryschoolict.com www.kidrex.org

The risks
The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people. Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. At Moston Lane we are committed to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk.

The technologies
New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or
- MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com,
- http://www.miniclip.com/games/en/, http://www.runescape.com/)
- Music download sites (Popular http://www.apple.com/itunes/, http://www.napster.co.uk/ http://www-kazzaa.com/, http://wwwlivewire.com/)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

Although the majority of these are not used in school, staff and children should be aware of the risks involved when using these technologies.

Roles and Responsibilities
E-Safety is recognised as an essential aspect of strategic leadership in this school and the headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the Policy is implemented and compliance with the Policy monitored.

Our ICT Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP). The school's e-Safety coordinator ensures the Headteacher is updated as necessary.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a
'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as digital cameras;
- Publication of pupil information/photographs and use of website;
- eBullying / Cyberbullying procedures;
- Their role in providing e-Safety education for pupils

System Safety Measures

Surfing the Web
Aimless surfing should never be allowed. Pupils should be taught to use the internet in response to an articulated need e.g. a question arising from work in class. Search engines can be difficult to use effectively. The teacher will need to choose a topic with care, select the search engine and then discuss with pupils sensible search words, which should be tested beforehand.

Education Programmes:
Pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering and monitoring.

This school:

- ✓ Fosters a 'No Blame' environment that encourages pupils to tell a teacher/responsible adult immediately if they encounter any material that makes them feel uncomfortable ;
- ✓ Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor or click on hector and report the URL to the teacher or ICT coordinator;
- ✓ Has a clear, progressive e-safety education to be taught throughout all key stages, built on LA / LGfL / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience.
- ✓ iPad rules and Sids Top Tips to be displayed in every class' computer area and the computing suite.
- ✓ To STOP and THINK before they CLICK
- ✓ To expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
- ✓ To discriminate between fact, fiction and opinion;
- ✓ To develop a range of strategies to validate and verify information before accepting its accuracy;
- ✓ To skim and scan information;
- ✓ To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- ✓ To know some search engines / web sites that are more likely to bring effective results;
- ✓ To know how to narrow down or refine a search; [for older pupils] to understand how search engines work;
- ✓ To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- ✓ To understand 'Netiquette' behaviour when using an online environment such as a 'chat' / discussion forum, i.e. no bad language, propositions, or other inappropriate behaviour;
- ✓ To not download any files – such as music files – without permission;
- ✓ To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos;
- ✓ To have strategies for dealing with receipt of inappropriate materials.

- ✓ Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- ✓ Makes training available annually to staff on the e-safety education program;
- ✓ Runs a rolling programme of advice, guidance and training for parents, including:
- ✓ Information in safety leaflets; in school newsletters; on the school web site;
- ✓ Demonstrations, practical sessions held at school;
  Suggestions for safe Internet use at home;
- ✓ Provision of information about national support sites for parents.

How will e-mail be managed?

Technology Safety:

Procedures
In the school context, e-mail should not be considered private and most schools, Moston Lane Community Primary School reserve the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation. The use of email in the school is limited to the use of accounts on the school domain within the school network. Personal e-mail addresses, such as Hotmail are blocked by the school system. Pupils will have class based email addresses which allow them to send and receive messages to and from the wider world, need to be carefully allocated to appropriate situations. All lessons that involve children sending or receiving emails must have full planning approved by the computing coordinator.

This school:

- ✓ Does not publish personal e-mail addresses of pupils or staff on the school website.
- ✓ We use anonymous or group e-mail addresses.
- ✓ If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we contact the police.
- ✓ Accounts are managed effectively, with up to date account details of users.
- ✓ Pupils are introduced to, and use e-mail as part of the ICT scheme of work.
- ✓ Pupils are first introduced to principles of e-mail through closed 'simulation' software e.g. I am learning.
- ✓ Pupils are taught about the safety and 'netiquette' of using e-mail i.e.

- Do not to give out their e-mail address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer;
- That an e-mail is a form of publishing where the message should be clear, short and concise;
- That any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
- To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- The sending of attachments should be limited;
- Embedding adverts is not allowed;
- That they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
- Not to respond to malicious or threatening messages,
- Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
- Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- That forwarding 'chain' e-mail letters is not permitted;

- ✓ Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.
- ✓ Staff sign the appropriate LA / school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Using Digital Images and Video Safely
Developing safe school web sites
The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety.computing coordinator to oversee / authorise the website's content and check suitability. It should be clear who has authority to upload content into sections of the website.

Use of still and moving images

Procedures:
Use excerpts of pupils' work such as from written work, scanned images of artwork or photographs of items designed and made in technology lessons. This allows pupils to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of pupils.

Links to any external websites should be thoroughly checked before inclusion on a school website to ensure that the content is appropriate both to the school and for the intended audience. Remember that the content of websites can change substantially, even in a short space of time. Check all links regularly, not only to ensure that they are still active, but that the content remains suitable too. Text written by pupils should always be reviewed before publishing it on the school website. Make sure that the work doesn't include the full name of the pupil, or reveal other personal information, such as membership of after school clubs or any other details that could potentially identify them. Although it may seem obvious, check that pupils' work doesn't contain any statements that could be deemed defamatory. Ensure also that the school is not infringing copyright or intellectual property rights through any content published on the website. For example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought.

Technical:
Digital images / video of pupils need to be stored securely on the school network and old images deleted after a reasonable period. When saving pictures, ensure that the image file is appropriately named. Do not use pupils' names in image file names or in <ALT> tag references when published on the web. *[An ALT tag is the HTML text describing a displayed image, used mostly for reasons of accessibility, since the tag can be voiced by screen readers].*

1
Education:
Ensure staff and pupils know who to report any inappropriate use of images to and understand the importance of safe practice. Staff and pupils also need to understand how to consider an external 'audience' when publishing or presenting work. In this school:

- ✓ The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- ✓ Uploading of information is restricted to SLT, Computing coordinator, Website lead teacher.
- ✓ The school web site complies with the school's guidelines for publications;
- ✓ Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- ✓ The point of contact on the web site is the school address and telephone number.
- ✓ Home information or individual e-mail identities will not be published;
- ✓ Photographs published on the web do not have full names attached;
- ✓ We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- ✓ Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted when children leave the school – unless an item is specifically kept for a key school publication;
- ✓ We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- ✓ We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- ✓ Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;

- ✓ Pupils are only able to publish to their own safe' KidBlog in school;
- ✓ Pupils are taught about how images can be abused in their eSafety education programme as part of the national curriculum.

How will infringements be handled?
Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

Students
Category A infringements:
- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites.
- **Sanctions reffered to computing coordinator.**

Category B infringements
- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups
- Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it
- **Sanctions: referred to Class teacher, e-safety Coordinator / removal of Internet**
- **Access rights for a period / contact with parent.**

Category C infringements
- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material
- **Sanctions: as category B and referred to deputy head.**

Other safeguarding actions
If inappropriate web material is accessed:
1. Ensure appropriate technical support filters the site

Category D infringements
- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute
- Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion / removal of equipment / refer to Community Police Officer / LA e-safety officer

Other safeguarding actions:
1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider

Staff

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network
- **Sanction - referred to line manager / Headteacher. Warning given.**

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.
- **Sanction - Headteacher.**

Tackling extremism and radicalisation

As a school we are fully committed to safeguarding against radicalisation and extremism. The aim is to protect individuals against radicalisation, or being exposed to extremist views, by identifying who they are and providing them with support. We are trained to recognise or identify safeguarding issues (Please see extremism and radicalisation policy).

Indicators:

- Increased usage of social media.
- Secretive usage of social media.
- Attempting to access inappropriate websites.
- Attempting to keep online activity secret.
- Attempting to keep online peers secret.
- Usernames or avatars that relate to a particular group.
- Public comments that relate to a group or cause.

All incidents will be investigated by computing co-ordinator/SLT alongside the safeguarding team. Every incident will be referred to a member of the safeguarding team.