

Moulton School and Science College e-Safety policy

1 Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Moulton School we understand the responsibility to educate our students 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, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

2 Rationale

The use of the Internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain therefore it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children use these technologies. These risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the Internet or any mobile device.
- Viruses.
- Cyber-bullying.
- On-line content which is abusive or pornographic.

It is also important that staff are clear about the procedures, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

Whilst we will endeavour to safeguard against all risks, we acknowledge we may never be able to eliminate them completely. Any incidents that may arise will be dealt with quickly and according to policy to ensure students continue to be protected.

This policy also aims to inform how parents/carers and students are part of the procedures and how students are educated to be safe and responsible users so that they can make good judgements about what they see, find and use. The term “e-safety” is used to encompass the safe use of all on-line technologies in order to protect students and staff from potential and known risks.

Schools are increasingly recognising the benefits of technology – and particularly Web 2.0 technologies – as an essential aspect of productive and creative social learning. However, in doing so we are finding that a blocking and banning approach which merely limits exposure to risk is no longer a sustainable approach. Children will experiment online, and while their confidence and enthusiasm for using new technologies may be high, their understanding of the opportunities and risks may be low, alongside their ability to respond to any risks they encounter.

We now need to focus on a model of empowerment: equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks, wherever and whenever they go online. An effective AUP can help to establish, and reinforce, safe and responsible online behaviours.

1. Aims

- To ensure the safeguarding of all students within and beyond the school setting by detailing appropriate and acceptable use of all on-line technologies.
- To outline the roles and responsibilities of everyone: students, staff, parents/carers
- To ensure staff are clear about procedures for misuse of any on-line technologies both within and beyond the school setting.
- To develop links with parents/carers ensuring input into policies and procedures with continued awareness of benefits and potential issues of on-line technologies.

3. Roles and responsibilities of the school

As e-Safety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The e-Safety Co-ordinator in our school is the Head of ICT. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety Co-ordinator to keep abreast of current issues and guidance through organisations such as Northamptonshire LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Headteacher/e-Safety Co-ordinator and all governors 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 agreements for staff and students, is to protect the interests and safety of the whole school community. It is linked to the following school policies: Child Protection, Health and Safety, Home-School Agreements, and Behaviour for Learning (including the Anti-Bullying Policy).

e-Safety skills development for students

- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.
- The e-Safety policy will be introduced to the students at the start of each school year.
- e-Safety posters will be prominently displayed in all areas of the school where ICT is used.
- The school’s internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school will ensure that the use of internet derived materials by staff and by students complies with copyright law.

- We will endeavour to embed e-Safety messages across the curriculum whenever the Internet and/or related technologies are used.

e-Safety skills development for staff

- All staff will be given access to the School e-Safety Policy and its importance explained.
- All staff will receive regular information and training on e-Safety issues
- New staff will receive information on the school's Acceptable Use Policy as part of their induction.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- Any staff member with an 'online identity' (e.g. in social networking sites) should ensure that access to this information is kept private and not shared with students.
- ICT technical support staff manage filtering systems and monitor ICT use in collaboration with the Headteacher.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential and that there should be no expectation of privacy when using any school ICT equipment (including laptops used off-site).
- All staff will be encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Appropriate use by staff

- Staff members have access to the Internet so that they can access age appropriate resources for their classes.
- They have a password to access a filtered Internet service and a personal email account and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.
- All staff will have access to the Acceptable Use Policy and a copy of the Acceptable Use Rules, which then need to be signed, returned to school to keep under file with a signed copy returned to the member of staff.
- The Acceptable Use Rules will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

4. Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- School ICT systems security will be reviewed regularly and in light of any new guidance issued by the LA, government or Becta.
- Passwords and network/MIS/school email user names will be kept safe and secure.

5. E-mail

The use of email within school is an essential means of communication for both staff and students. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an email in relation to their age and good 'netiquette'.

Staff

- Staff are issued with EMBC email accounts (xxx.yyy@moultonschool.co.uk) to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Staff may access personal email accounts during break times or before/after school.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, “the views expressed are not necessarily those of the school”. The responsibility for adding this disclaimer lies with the account holder.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations, parents or students are advised to cc. the Headteacher, line manager or other designated account.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Staff must inform the e-Safety co-ordinator/ line manager if they receive an offensive e-mail.
- Staff are advised not to share personal email addresses with students, but may share their EMBC email account where appropriate.

Students

- Students are issued with EMBC email accounts (@moultonschool.co.uk) to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Students will be introduced to email as part of the ICT Scheme of Work.
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- It is the responsibility of each student to keep their email password secure.
- For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- The forwarding of chain letters is not permitted.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

6. Student’s images and work

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

On a child’s entry to the school, we shall seek the preference of all parents regarding the use of their child’s work/photos in the following ways:

- on the school web site
- on the school’s VLE
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school’s communal areas
- in display material that may be used in external areas, i.e. an exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

Thereafter, in the autumn term each year, parents and sixth form students will be asked to confirm their preferences. Reports can then be generated of the names of students whose parents would prefer them not to be photographed.

Only the Web Manager has authority to upload to the site.

Taking of Images

- With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the students device.
- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students names will not be used anywhere on the school website or other on-line space in association with photographs or video, unless express permission has been granted by parents/carers.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site.
- Work can only be published with the permission of the student and parents.

Storage of Images

- Images and videos of children are stored on the school's network
- Students and staff are not permitted to use personal portable media for long-term storage of images (e.g. USB sticks, mobile phones, digital cameras) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network/ VLE.
- The data manager has the responsibility of deleting the images when they are no longer required, or the student has left the school.

Webcams and CCTV

- The school uses CCTV for security and safety. Its use falls under the School's Data Protection Policy
- We do not use publicly accessible webcams in school.

Video conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- Students should ask permission from the supervising teacher before making or answering a video conference call.
- All students are supervised by a member of staff when video conferencing
- No part of any video conference is recorded in any medium without the written consent of those taking part.
- Video conferencing should, if possible, use the EMBC 'Click-to-meet' educational broadband network to ensure quality of service and security rather than the Internet.

7. Social networking and personal publishing

If used responsibly both outside and within an educational context, Web 2 technologies, including social networking sites, can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to block/filter access to social networking sites.
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students are always reminded to avoid giving out personal details on such sites which may identify them, their friends, or where they are (full name, address, mobile/ home phone numbers, school details, IM/email address, specific hobbies/ interests).
- Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our students are asked to report any incidents of bullying to the school.
- Students and parents will be advised that the use of social network spaces outside school brings a range of dangers for students.
- Staff will be given advice on the personal use of social networking

8. Managing filtering and monitoring

Filtering

- The school will work in partnership with the LA, DfE and internet provider to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the e-Safety Coordinator or the Network Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- If staff or students come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator. Sites can be referred to the EMBC team for global blocking if required, or local blocking can be performed on-site through appropriate Internet management software.

Monitoring

- Logs of Internet access will be kept and monitored by the ICT technical support team, with all relevant issues reported to the e-Safety Co-ordinator/Headteacher.

9. Managing emerging technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are also familiar to students outside school. They often provide a collaborative, well-known device with possible Internet access and thus open up risk and misuse associated with communication and Internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately:

- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time when the device must be switched off.
- This technology may be used, however, for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- The appropriate use of VLE/Learning Platforms will be discussed as the technology becomes available within the school.

10. Protecting personal data

Personal data will only be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the School's Data Protection Policy.

11. Policy Decisions

(a) Authorising Internet access

- All staff must read and sign the Staff AUP before using any school ICT resource.
- Parents will be asked to sign the AUP for their child to use the Internet as part of the induction process. Children are asked to counter-sign the AUP after discussion with parents/carers.
- The school will maintain a current record of all staff and students who are not granted access to school ICT systems.

(b) Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school can not accept liability for the material accessed, or any consequences of Internet access.
- The school will monitor and audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

(c) Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse should be referred to the Headteacher.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.
- Students and parents will be informed of the complaints procedure.
- Students, parents and staff will be informed of consequences for misusing the Internet.

12. Communicating the policy

(a) Introducing the e-safety policy to students

- Students will receive a copy of the Acceptable Use Rules on entry to the school to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules.
- It is expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.
- The school will keep a record of the signed forms.
- e-Safety rules will be posted in all rooms where computers are used and discussed with students regularly.
- Students will be informed that network and Internet use will be monitored and appropriately followed up.

- Students will be informed of the availability of a “Report Abuse” button (on the school ICT website and other sites) should there be a concern of inappropriate or malicious contact made by someone unknown. This provides a safe place for children and young people to report an incident if they feel they cannot talk to a known adult.
- e-Safety training will be embedded within the ICT scheme of work.

(b) Enlisting parents’ support

- Parents’ attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site.
- Parents with any concerns about e-Safety are encouraged to contact the school for further guidance and support.
- Parents sign the Parent’s Consent Form on an annual basis after sharing our age-appropriate safety rules with their child.