Moor House School & College

E-**S**afety Policy

Version:	3
This Version Dated:	January 2016
Most Recently Reviewed By:	M. Crowhurst / H.Middleton
Status:	Draft / Agreed by Staff / Sent to ECM/ Approved by FGB
Who needs to read this?	All staff who use technology in lessons or who supervise students when they are using technology.
Next Review Date:	January 2017

CURRENTLY BEING REVIEWED

Moor House is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment

Introduction and Guiding Principles

E-safety refers to the safe use of information systems and electronic communications. E-safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

- E-safety concerns the safeguarding of children and young people in the digital world.
- E-safety emphasises learning to understand and use new technologies in a positive way.
- E-safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.
- E-safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

Policy Summary

- Ensure everyone at MHS&C knows how to use the Internet safely.
- Create an environment that does not tolerate Cyber-Bullying
- Provide on-going training to students and staff on how to use the Internet safely
- Provide age and competency level specific access to internet content using MHS&C technology
- Provide the framework for 3rd party technology to be used at MHS&C
- Ensure everyone at MHS&C knows how to escalate breaches in the policy
- Ensure the school and college has the appropriate monitoring in place to review Internet access and usage

The Responsibility of the School & College and Staff in Supporting E-safety .

- To ensure that all approaches and strategies utilised to educate students at Moor House School & College and develop their awareness of safe online practices will take into consideration their speech and language impairment.
- Staff will guide students to online activities that will support the learning outcomes planned for the students' age and maturity.
- The school and college's Internet access includes content filtering which assists in filtering out potentially inappropriate content and monitors usage to provide audit trails.
- Students will be taught about acceptable internet use and given clear guidance.
- Students will be educated in the safe and effective use of the internet for research purposes, including the skills of navigation, knowledge location, information retrieval and evaluation.
- Students will be made aware of the dangers of giving out personal or private information online.
- Students will be taught to be critically aware of the reliability of materials they access/view online and be shown how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information used and respect copyright when using material in their own work.
- Students will be taught how to report inappropriate Internet content.
- Staff may contact students to relay information via official school channels: school e-mail, telephone and post. College staff use school mobile phones to contact students during staff working hours.
- Staff should always use school e-mail addresses for school-related activities.

- Staff must not deliberately contact students for matters that are unrelated to school. Communications between staff and students should not occur through social networking sites, online video or audio calls, personal e-mail addresses or exchange chat messages, unless with the express and specific documented consent from the Senior Management Team. Classroom practitioners wishing to use Social Media tools with students as part of the school curriculum should risk-assess the websites before use and check the site's terms and conditions to ensure the site is suitable.
- Any e-safety incident that involves any student at Moor House School & College will be dealt with as a child protection issue following procedures outlined in the school's Child Protection, including Safeguarding, Policy
- In addition, the school and college will ensure there are specifically trained staff across the departments to whom concerns can be raised with regard to e-safety. These staff members are trained by a special Police service known as the Child Exploitation Online Protection Service (CEOP). (See appendix for names of current staff).
- The school & college will be sensitive to Internet related issues experienced by students out of school, e.g. social networking sites, and offer appropriate advice.

The Responsibility of Students in Supporting E-safety

- Students must tell a member of staff immediately if they receive an offensive e-mail or other form of electronic communication (refer to Discrimination Policy).
- Students must not reveal personal details of themselves or others in e-mail communication or on social networks.
- Students must never arrange to meet anyone they have met through the internet, without specific permission to do so from their parent or guardian.
- Students must not attempt to contact staff outside of school, via social networking sites, online video or audio calls, personal e-mail addresses or exchange chat messages. School e-mail is the most appropriate form of electronic communication with staff.
- Students should inform a member of staff if they receive any incoming e-mails from unknown sources, avoid replying to the sender or forwarding the content, and avoid opening the attachments as these may contain computer viruses.

The Responsibility of Parents and Guardians in Supporting E-safety

- Parents and guardians should work in partnership with Moor House and its staff in relation to any issues pertinent to e-safety in the spirit of collaboration and to best protect the wellbeing of the child.
- Where possible, parents and guardians should implement parental control systems to limit Internet access to safe content only.

E-safety Management within the School and College Community

Information System Security

- The security of the school and college information systems will be reviewed regularly by the IT Manager. A report will be submitted on a termly basis to SMT and the Finance Committee regarding actions taken and any recommendations.
- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.

- Technology that is not under the jurisdiction of Moor House School and College may not access the network unless agreed by the Senior Management Team. Where staff require remote access to the network this can only be authorised by a member of SMT.
- Students are permitted to copy their personal work on to portable storage devices to enable work at home and to practise backing up their work. Within the school environment, this process is supervised by the ICT teacher. Students will be prevented from downloading software to school computers, via their user privileges status. Staff will determine whether a download request is deemed suitable and necessary. A request can then be made, via the member of staff, to the IT Helpdesk to be put into effect.
- College students are encouraged to copy their work to portable storage devices for use at partner colleges and at home. They are supported by staff where necessary but independence in this area is encouraged.
- Unapproved software will not be allowed in students' user areas or attached to e-mail.
- All users of the system must agree to the school's Acceptable Use Policy (AUP).

Management of E-mail

- Staff will use only official school provided e-mail accounts to communicate with students and parents/carers, as approved by the Senior Management Team.
- Staff should not use personal e-mail accounts during their school working hours, unless done so during their allocated break times/off duty, when students are not present/in the vicinity.
- Access to external e-mail accounts will be blocked if used at inappropriate times and must not be used to contact parents or students.
- Students may use only official school and/or link college e-mail accounts provided whilst at school.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. The appropriate disclaimer notice should be attached.
- The forwarding of chain messages is not permitted.
- Staff must immediately tell their Line Manager if they receive offensive e-mail.

Management of School Website Content

- The contact details on the website should be the school and college address, e-mail and telephone number. Staff or students' personal information will not be published.
- SMT will take overall editorial responsibility for the school website, to review content and ensure that it is accurate and appropriate.
- The school and college website will comply with the school and college's guidelines for publications including respect for intellectual property rights and copyright.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of students are electronically published.
- Students' work can only be published with their permission or that of their parents/carers.

Management of Social Networking and Personal Publishing

- The school will control access to social media and social networking sites through the school and College's filtering system and list of approved websites. However, College students have access to

social networking sites as a privilege which may be withdrawn without notice if used inappropriately.

- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to 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 e-mail addresses, full names of friends, specific interests and clubs etc. However, an email address may be provided if deemed appropriate by the ICT teacher for example to sign up for presentation software such as Prezi
- Students should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location for example house number, street name or school.
- Classroom practitioners' official blogs, wikis etc. should be password protected and run from the school website or approved school communication channels.
- Staff wishing to use social media tools with students as part of the curriculum should risk assess the site before use and check the sites terms and conditions to ensure the site is suitable. Documented consent must be given by the Senior Management Team before use.
- Classroom practitioners should use official e-safe networking spaces available online. Specific zones can be set-up within these networking environments to restrict access to Moor House students and staff only. Staff must not run social network spaces for student use on a personal basis.
- Students should be advised on security and encouraged to set safe passwords, deny access to unknown individuals and instructed how to block unwanted communications, if or when the need arises. Students should be encouraged to communicate to known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.

Management of Content Filtering

- The School & College will define the requirements for access control strategy to suit the age and curriculum requirements of the students. The IT Manager will implement the approach agreed.
- All breaches of Content Filtering Policy will the reported to the H&S Committee for review.
- The IT Manager will ensure that regular checks are made to ensure that the filtering methods continue to be effective.
- Any online material that the school believes is illegal will be reported to appropriate agencies such as Surrey Police, the IWF (Internet Watch Foundation) or CEOP (Child Exploitation and Online Protection Centre)**.**
- The school and college's internet access will include filtering appropriate to the age and maturity of students.
- If students discover unsuitable sites, they must report these to a member of staff. Staff will note the URL (website address) and report it immediately to the IT Manager and carbon copy the e-mail to the e-safety Coordinator and Designated Safeguarding Lead.
- Staff can make a request to the IT Manager to unblock sites which they deem appropriate in their professional capacity for student or staff viewing.
- Student access levels will be reviewed as necessary, to reflect the age of the students, educational requirements and changes to the curriculum.

Management of Emerging Technologies

- Emerging technologies will be examined for educational benefit and discussed with the Assistant Head Teachers, before they are introduced for use in school.

- The school utilises wireless technology. A public wireless network is utilised in the college. Students are permitted access to this facility, but the password is confidential and only privileged to staff. (Refer to the use of wireless, infra-red and Bluetooth communication technologies in the AUP.

Policy Decisions

The School and **C**ollege will:

- Maintain a current record of any person who is granted access to the school's electronic communications. All staff and governors must read and sign the Acceptable Use of Technology and Networks Policy (AUP) before using any school and college ICT resource.
- Take all reasonable precautions to ensure that users access only appropriate material.
- Audit ICT use to establish if the E-Safety Policy is adequate and that the implementation of the E-Safety Policy is appropriate.
- The school and college recognises that withdrawal of computer and Internet facilities for a student could have a detrimental effect on that student's progress and coursework grades. However the school will withdraw access in cases where it is deemed necessary.
- Staff, students and/or their parents/ carers/ guardians will be expected to sign an 'Acceptable Computer Use Agreement' declaring that they will abide by the expectations set out by the school and college. Parents will be informed that students will be provided with filtered Internet access.

Management of E-Safety Complaints

- Complaints of Internet misuse will be dealt with under the school's Complaints Procedure. Any complaint about staff misuse must be referred to the Principal. Students and parents will be informed of the complaints procedure. Parents and students will need to work in partnership with staff and the school to resolve issues.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Education Safeguards Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the Moor House's disciplinary and/ or child protection procedures. All E-Safety complaints and incidents will be recorded by the E-Safety Officer — including any actions taken.
- All members of the school and college community will be taught or trained about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community. This forms part of the initial child protection training.

Management of Cyber bullying

Please refer to Anti-Bullying Policy.

Communicating this E-Safety Policy

- Staff will have training in e-safety to raise awareness of the importance of safe and responsible Internet use.
- E-safety rules will be taught to every student and will be posted in ICT areas.
- An e-safety module will be included in the PSHE and/or ICT programmes covering both safe school and home use (see PSHE and ICT policies).
- All users will be informed that network and Internet use will be monitored.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum.
- All Staff will sign to acknowledge that they have read and understood the e-safety policy and agree to work within the agreed guidelines.

- Staff that manage filtering systems or monitor ICT use will be supervised by a member of the Senior Management Team and have clear procedures for reporting issues.
- Parents have the opportunity to receive information and training opportunities about e-safety. The Moor House E-Safety policy will be made readily available to parents on the website and e-mails will be sent to parents each year referencing the policy. Parents/carers are invited to annual parent workshops in order to receive information on E-Safety.

Review

- This policy will be formally reviewed annually by a multidisciplinary team of staff to check that it continues to represent our aims and practices. This team will be led by the Assistant Head Teachers and the Head of Residential Care.
- All students will be asked, through the School Council or Moor House College Forum, about their views on the use of Internet in the school and their views on this policy so that they may suggest amendments or improvements.
- Heads of Department will also monitor the success of this within their departments throughout the year and provide feedback to the Senior Management Team if they have concerns about consistency of application.

APPENDIX 1

This policy links with the following other policies, which should also be read:

- Acceptable Use of Technology and Networks Policy
- Anti-Bullying Policy
- Child Protection, including Safeguarding, Policy
- Complaints Policy
- Staff A to Z

E-Safety Officer:
Matthew Crowhurst

Designated Safeguarding Leads:
Helen Middleton
Sue Brady
Nick Hart
Madeleine Van Niekerk
Daniel Carroll
Susie Simpson

Current Staff with Additional Training in CEOP:

Matthew Crowhurst – Teacher
Ercan Arga- Residential Care Worker
Susan Pope – Speech Therapy Assistant
Chris Osborne - Teacher

Sources:

Child Exploitation Online Protection Website
http://www.ceop.police.uk

Schools' E-safety Policy Generator https://www.policy.e-safety.org.uk/default.cfm?pid=10&pcid=2

Additional Contact on E-Safety Issues:

Ian McGraw

Education Safeguarding Coordinator

Contact Tel: 01483 518158

Mobile: 07772 009477

E-mail: ian.mcgraw@surreycc.gov.uk / secure e-mail: ian.mcgraw@surreycc.gcsx.gov.uk

APPENDIX 2

Cyberbullying; Advice for head teachers and school staff

Ref: DFE – 00652-2014

PDF 195kb 6 pages

APPENDIX 3

Advice for parents and carers on cyberbullying

Ref: DFE 00655 – 2014

PDF 185kb 7 pages