Manor Green College E-learning and e-safety Policy - Applicable to staff and students

The policy

The aim of our e-learning safety policy is to outline the procedures that we have put in place to ensure that our pupils and staff can make best use of the ICT facilities available to them in a safe and secure way. The overarching principle for this document is to enhancing student experience, student independence and resilience and student attainment.

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, and computing.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

The e-Safety Policy is part of the ICT Policy and School Improvement Plan and relates to other policies including those for behaviour, personnel, social and health education (PSHE) and citizenship. This policy refers to the pupil and staff AUP (Acceptable Use Policy (of the network)) and also the Data Security Policy which should be read in conjunction with this policy. In line with GDPR (See the school policy on GDPR) we have now encrypted staff laptop computers and prevented, removing data from the laptops. This means all sensitive data is protected.

All students have e-safety awareness information in their planners, and both the ICT and PSHE cover how to be safe online in their curriculums. The PSHE coverage is adaptive to the needs of students and responds to the additional pastoral needs of pupils as well as the standard curriculum. We invite external agents such as CEOP to run assemblies and workshops with our students.

This e-Safety Policy has been written by the school, to build on the AUP policy and government guidance. It will be reviewed bi-annually.

1. Teaching and learning
Why is Internet use important?

- The purpose of Internet use in the 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 use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. Manor Green College has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and sources and critically, to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in the *National Education Network* which connects all UK schools;

- Educational and cultural exchanges between pupils world-wide; ocational, 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 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 between Kingsford, the Local Authority and DfE;
- Access to learning wherever and whenever convenient.

HOW CAN INTERNET USE ENHANCE LEARNING?

The School aims to develop effective practice in Internet use for teaching and learning. Teachers, tutors, the Librarian and other support staff help pupils to learn how to distil the meaning from the mass of information provided by the Internet. Often the quantity of information is overwhelming and staff may guide pupils to appropriate websites. Internet searching skills is part of the ICT curriculum. Above all pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet.

- The School Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils. The filter is set by Exa and Surfprotect sub contractors of (JSPC) and not the local authority.
- Pupils are explicitly taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. This is implemented more so for FE students.
- Staff guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

The ICT KS3 curriculum will enable students to become mature internet users by incorporating all the above. The PSHE curriculum assists students in helping them to assess risk in handling and sharing their personal information online as well as the meaning and consequences of cyber-bullying, apps that store personal details, and social media pitfalls.

2. MANAGING INFORMATION SYSTEMS

HOW WILL INFORMATION SYSTEMS SECURITY BE MAINTAINED?

The School's Acceptable Use Policy is displayed every time they log on and in the initial agreement signed by parents.

Pupils must accept the AUP before access to the computer is granted. In their ICT lessons pupils are taught about good ICT security practice. Sanctions are in place for pupils who break the School's AUP. For School staff, strict and clear guides are in place for use of electronic equipment. There is also an appendix which highlights responsibility when using social media and other media apps with respect to mentioning work related comments.

There is a common understanding and duty to preserve the security and integrity of the ICT system at Manor Green College.

- Workstations are secured (e.g. C: Drive) and network drives are only available with the correct permissions
- Physical access to servers is restricted.
- The server operating system is secured and kept up to date.
- Virus protection for the whole network is installed, current and continually updated.
- Access by wireless devices is limited to devices authorised by the network manager
- A robust backup system is in place

The School's internet connection is via Exa Networks managed also by JSPC Computer Services to ensure compliance with the security policy. Firewalls and switches are configured to prevent unauthorised access to known sites that are deemed unsuitable. The security of data is covered in more detail in the Data Security Policy (where is this). The following points cover some of the main issues regarding data security:

- Personal data sent over the Internet will be encrypted or otherwise secured.
- Data relating to pupils will not longer be carried on USB Pen ~~drives must be encrypted (teacher must be taught how to do this, I will liaise with (SB) on this~~
- Unapproved system utilities and executable files are not allowed in pupils' work areas or attached to e-mail.
- Files held on the Schools' network will be regularly checked.
- The network manager will review system capacity regularly.

How will e-mail be managed?

Pupils are taught to use e-mail during functional skills, which will be taught through Years 10 and 11 and in FE. Other emails have been disallowed for other year groups.
Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission. **Staff must use their School e-mail address for all professional correspondence. Staff must not use the school email to express their view or opinions on outside issues, politics, nor endorse any causes.**

- Access for students in the School to external personal e-mail accounts is blocked.
- (Some students do have access to Google mail, and whilst this is not encouraged during lessons this could be an opportunity for teaching and learning to take place.)
- E-mail sent to external organisations should be written carefully, in the same way as a letter is written on School headed paper.
- Most recent disclaimer message has now been added to staff emails 2018 in line with GDPR guidelines
- The forwarding of chain letters is not permitted by any users and will be challenged by SLT.

How will published content be managed?

- The contact details on the website will be the School address, e-mail and telephone number. Staff or pupils' personal information are not be published. (OA will send an email to staff on how to save a signature)
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. There is a separate document relating to emails by staff.
- The website will comply with the School's guidelines for publications including respect for intellectual property rights and copyright.

Can pupil's images or work be published?

Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Written permission from parents or carers will be obtained before images of pupils are electronically published. List held by office of pupils who have not given permission for photographs. Parents have consented the use of photos as per conditions in the student's notes on SIMs.

How Will Social Networking and Personal Publishing Be Managed?

- The School has blocked access to all social networking sites for students, access to these sites via proxy servers is specifically outlined in the AUP.
- Pupils are advised never to give out personal details of any kind which may identify them and / or their location. This includes real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils are advised not to place personal photos on any social network space. They are taught to consider how public the information is and consider using private areas. Advice is given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students are taught to invite known friends only and deny access to others.

How will filtering be managed?

Staff are able to add blocked sites to our 'allow' list if the member of staff deems that they are suitable and is agreed by the Head of ICT (Patrick Cambridge). If staff or pupils discover unsuitable sites, the URL must be reported to the Network Manager immediately (Fred Fisher) or (Patrick Cambridge). Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. In addition to robust filter the school also has the option to block or release sites with almost immediate effect.

How can emerging technologies be **managed**?

- Mobile phones will not be used by pupils during lessons or formal school time, unless part of their lesson. Teachers wanting to use mobile phone technology in their lesson must first discuss the use with their LAL.

- The sending of abusive or inappropriate text messages is forbidden and covered in the school's behaviour policy as bullying.
- Staff will be issued with a School phone where contact with pupils is required. Staff must not give their personal mobile number to pupils, unless this has been agreed by the Head Teacher or SLT, and the CPO has been informed of the reasons as to why this is necessary.

How should personal data be protected?

For more information on this please see our Data Security Policy. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

3. Policy Decisions

How will Internet access be authorised?

The School maintains a current record of all staff and pupils who are granted access to the School's electronic communications. All staff must read and sign the 'Staff Information AUP' before using any School ICT resource. All pupils must agree to abide by our Acceptable Use Policy each time they login. Parents of new Year 7 pupils are asked to sign and return a consent form for pupil access. Pupils who are mid-phase admissions or start at any other time of the year will have a consent form in their starter pack.

How will risks be assessed?

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The School addresses the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the School system.

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. Neither the School nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use.

The School audits ICT use to establish if our e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

In order to ensure that students are equipped to make safe decisions about their time online when away from school (where the filters and firewalls may not be as robust or in place) curriculum time is devoted to teaching safe searching and assessing the risks of sharing data so students can make good decisions.

.

How will e-safety complaints be handled?

Complaints of Internet misuse will be dealt with by The Network Manager and Head of ICT. Any issues of e-safety regarding pupils will be dealt with by the relevant Team leader and copies of all incidents will be sent to the Head's PA, and Mr. Cambridge, Head of ICT.

Any issues relating to breach of the Acceptable Use Agreement will be dealt with by the Head of ICT and the Network Manager. Any complaint about staff misuse will be referred to the Head Teacher.

- Sanctions regarding cyber-bullying are outlined in the School's anti-bullying policy
- Sanctions for breach of the AUP range between temporary removal of Internet access to temporary exclusion depending on the severity of the offence.

4. Communications Policy

How will the policy be introduced to pupils?

E-Safety is a crucial part of every pupils' education at the School. Currently the following are used to ensure pupils are aware of the issues:

- At least one assembly for each year group per year is on the topic of e-safety
- School AUP is displayed each time pupils log in
- The E-safety policy is available via the School's website
- Links to various E-Safety websites are on the School website
- Parents' evenings on topic of E-Safety Parentzone workshops / Website links.
- Posters around the School highlighting e-safety

How will the policy be discussed with staff?

- All staff will be made aware of the electronic version of the School e-Safety Policy and its application and importance explained.
- Staff are made aware that Internet traffic is be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use are supervised by senior management and have clear procedures for reporting issues. All breaches of E-safety policy should be reported to the Network Manager
- Staff training in safe and responsible Internet use and on the School e-Safety Policy will be provided as required.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School's e-Safety Policy in newsletters, the School brochure and on the School website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents is encouraged. This includes parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Workshops based on Parent zone will be available to help parents and carers help their children with online safety outside of school.
- Online safety and e-learning has now been exclusively incorporated into the ICT curriculum at all key stage levels. SLT and HOD have developed and agreed that one half term a year will be dedicated to teaching Internet Safety across the entire school. All teachers who are responsible for teaching ICT will also follow this scheme of work and use the CEOP learning programme and resources.
- Online assemble is given prominence passing the safety message across during this period of e-learning.
- A current subscription to Vodafone safety magazine and links with O2 shop in Crawley has meant the school has distributed to all children and their families, Online safety literature.

Next Review Date: Summer Term 2020

Reviewer: P Cambridge **September 2018**

This Policy was formally reviewed and ratified by the Governing Body on _26.9.18_________________

Signed:_____________________________________
Chair of Governors