APPENDIX E: Information & Communications Technology E-Safety Policy

1. Introduction

Kingston Maurward College recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners, staff and visitors to encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use.

Our approach is to implement appropriate safeguards within the College while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies.

In furtherance of our duty to safeguard learners, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care. This e-Safety policy should be read alongside other relevant College policies e.g. Safeguarding, Prevent, Acceptable Use, Anti Bullying, Disciplinary, Student Parent Guardian Code of Conduct and Staff Code of Conduct

2. Creation, Monitoring and Review

Consultation for the development of this policy was carried out at the ICT Committee and Student Council.

The impact of the policy will be monitored regularly with a full review being carried out at least once a year. The policy will also be reconsidered where particular concerns are raised or where an e-safety incident has been recorded.

3. Policy Scope

The policy applies to all members of the College community who have access to the College IT systems, both on the premises and remotely. This policy should be read in conjunction with the ICT Acceptable User Policies for staff and students and the staff Code of Conduct.

4. Roles and Responsibilities

All learners must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be their Course Manager or a member of the Student Welfare team (121@kmc.ac.uk or 01305 215121).

The College will try to ensure that students have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

All staff are responsible for ensuring the safety of learners and should report cases appropriately. Staff should report serious concerns to a member of the Student Welfare team and be aware that the Safeguarding team may be asked to intervene with appropriate additional support from external agencies.

When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved. However, information should only be shared with those who need to know.

Guidance on staying safe for learners may be found in Section 11.

Guidance on staying safe for staff may be found in Section 12.

5. Security

The College will do all that it can to make sure the College network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of College systems and information. Digital communications, including email and internet postings, over the College network, will be monitored.

6. Behaviour

Kingston Maurward College will ensure that all users of technologies adhere to the standard of behaviour as set out in the Acceptable Use Policy on Moodle.

Whether offline or online, communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes. These are available on Moodle.

Where conduct is found to be unacceptable, the College will deal with the matter internally. Where conduct is considered illegal, the College will report the matter to the police.

Guidance on staying safe for learners may be found in Section 11.

Guidance on staying safe for staff may be found in Section 12.

7. Personal Information

Personal information is information about a particular living person. Kingston Maurward College collects and stores the personal information of learners and staff regularly e.g. names, dates of birth, email addresses, assessed materials and so on. The College will keep that information safe and secure and will not pass it onto anyone else without the express permission of the learner or member of staff.

Staff must keep learners' personal information safe and secure at all times. When using an online platform, all personal information must be password protected. Where the personal data is no longer required, it must be securely deleted in line with the GDPR and the College's Data Protection policy.

8. Education and Training

With the current unlimited nature of internet access, it is impossible for the College to eliminate all risks for staff and learners. It is our view therefore, that the College should support staff and learners to stay e-safe through training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

For learners:

Full time learners will receive e-safety training as part of their group tutorial programme. Student Services staff will ensure that up-to-date information and relevant activities are available on Moodle to support this training. Course Managers will deliver the College's extremism tutorial as part of this programme. The tutorial is available from Moodle.

Part time learners will receive guidance on e-safety from their course teacher.

Residential students will receive additional training from the Wardening team, particularly those students who are vulnerable and at additional risk.

Work based learners will receive guidance on e–safety through their regular reviews.

Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

As part of their Student Welfare inductions, learners are told how to report e-safety concerns.

For staff:

E-safety training for staff is incorporated into the College's Safeguarding training that all new staff receive at induction. On an annual basis staff are updated in respect Keeping Children Safe in Education. This is reinforced at least every three years when staff are required to undertake refresher training. Key staff are required to attend update sessions every two years. All staff receive regular safeguarding updates annually by different methods. Staff are required to undertake appropriate training in relation to the Prevent agenda.

9. Incidents and Response

Where an e-safety incident is reported to the College this matter will be dealt with very seriously. The College will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their Course Manager or to a member of

the Student Welfare team. Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible.

Following any incident, the College will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident.

Concerns or incidents relating to extremism must be reported to a member of the child protection team and will then be referred, if appropriate, to the Channel process through the Safeguarding Referral Unit at Dorset Police.

10. Extremism and Radicalisation

Many extremist groups such as far right groups, animal rights activists and religious fundamentalists who advocate violence or other criminal activity use the internet as a means of recruiting young people. Because of their personal circumstances, some young people may be susceptible to these influences.

Staff need to be aware of those young people who are being targeted by or exposed to harmful influences from violent extremists via the internet. Young people should be warned of the risks of becoming involved in such groups and it should be against service policy to access such sites.

11. Guidance on staying safe online for students

Personal Safety

- Don't post any personal information online – like your address, email address or mobile number.
- Think carefully before posting pictures or videos of yourself. Once you've put a picture of yourself online most people can see it and may be able to download it - it's not just yours anymore.
- Sexting images of yourself even to someone you trust is dangerous as they could still end up being posted on the internet and going viral.
- Keep your privacy settings as high as possible
- Keep your username and password secure. Never give out or share your passwords
- Don't befriend people you don't know

- If you meet up with someone you have met online, arrange to meet them in a public place and tell someone where you are going and what time you expect to be back. If possible, take a friend with you.
- Remember that not everyone online is who they say they are.
- Be careful about joining organisations or groups without checking them out first. They may appear to be well-meaning but they could be trying to engage you in illegal or dangerous activities – for example, some political, religious or animal rights groups may want you to break the law in the name of their cause.
- Don't put anything online that you might later regret – remember that the Internet has a long memory
- If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website, turn off your computer if you want to and tell someone immediately. You can report it to your Course Manager or a member of the Student Welfare team.

Responsibilities towards others

- Think carefully about what you say before you post something online
- Be polite and responsible when you communicate with others. Do not use strong, aggressive or inappropriate language.
- Respect other people's views even if you don't agree with them
- Don't take photographic images and/or audio recordings of anyone or distribute them without their express permission
- Don't ask to use someone else's password details

Make sure that you comply at all times with the Acceptable Use Policy for Students which can be found on Moodle.

12. Guidance on staying safe online for staff

- All digital communications with learners must be professional at all times.
- Personal information, including contact information, should not be shared with students or their parents.
- Don't post anything that may compromise your professional role or bring the College into disrepute.
- Only use social media sites with students that are authorised by College. Make sure that at least one other member of staff has access to the forum you are using.
- Don't be friends or communicate on social networking sites with students[1] or their parents – keep work and home separate. If you are a manager or supervisor, avoid being friends with employees.
- Avoid texting – texts can be manipulated and students should not have access to your personal mobile number.
- Use College equipment if taking photos and be aware of posting photos publicly. You must seek students' permission before posting photos even on a College Facebook page.
- Avoid taking photographs or videos in a one-to-one situation and remember that you may be asked to justify any images in your possession.
- Don't put anything online that you might later regret – remember that the Internet has a long memory.
- Report any concerns so that they can be dealt with openly and effectively. You can refer them to your line manager, the Deputy Principal Learning & Performance or the Assistant Principal, Student Experience & Progression. If you are shown images that concern you, do not copy, print, download or forward those images.
- Make sure that you comply at all times with the Acceptable Use Policy for Staff which can be found on Moodle.

[1] If your child has friends who may be students at KMC, restrict your privacy settings so that his/her friends cannot see your pages and you cannot see the friends' pages.

- Report concerns about students or other staff to the Safeguarding team if you believe that they are at risk of sexual grooming, bullying, sexting or radicalisation.

- Remember that education is key – help your students to be aware and stay safe online.

13. Feedback and Further Information

Kingston Maurward College welcomes all constructive feedback on this and any other College policy. If you would like further information on e-safety, or wish to send us your comments on our e-Safety Policy, then please contact: Nicky Porter, Assistant Principal Student Experience & Progression on 01305 215118 or nicky.porter@kmc.ac.uk