APPENDIX B: Information & Communications Technology Acceptable Use Policy for Students

Policy Statement

Kingston Maurward College has invested, and will continue to invest, in the necessary ICT resources to ensure that you are able to make the most of the advantages offered by this technology.

We are committed to maintaining up to date facilities and will ensure that all students have access to the necessary equipment in order to aid their studies. Information & Communications Technology facilities should only be used for college/course related work except in certain circumstances outlined below.

This policy is to be regarded as a code of conduct for all students. Failure to observe is likely result in action being taken in accordance with the College's Student disciplinary procedure.

Any student, who experiences problems concerning abuse of Information Technology facilities, should in the first instance approach their Course Tutor, Course Manager or Programme Lead.

In order to comply with the latest legislation, the College has the right to and does monitor all computer equipment that it either owns or leases, and any data that is either stored on or passed through its computer systems. This also includes monitoring of printing, emails and internet traffic.

All student internet usage is monitored and search requests / access to websites of concern are reported to the Principal and the Assistant Principal Student Experience & Progression; where the College is concerned, this is likely to result in you meeting with your Course Manager to discuss your internet usage and habits.

2 Scope

This policy relates to the use of all ICT related facilities whether owned or leased by Kingston Maurward College.

3 Computer Systems, Software & Data

3.1 No software whatsoever is to be downloaded or installed on any College computer. The installation of officially recognised licensed software must be authorised and carried out by IT Support Team

3.2 The use, or possession, of unlicensed copies or "pirated" versions of software is illegal and, therefore, strictly prohibited on College premises.

3.3 The use of computer games is strictly prohibited on College computers.

3.4 All ICT equipment must be treated with due care and attention at all times.

3.5 Any computer problems, faults or viruses must be reported to a member of staff who should inform IT Support Team immediately.

3.6 Only College/course related data should be stored on College computers.

3.7 The College will not be held responsible for the loss of any data from its computers. Users are therefore reminded to keep separate back-up copies of all valuable work.

3.8 On occasions it may be possible to for students to loan college hardware and/or software. On these occasions, students will be asked to read and sign the relevant agreements.

4 Internet

4.1 Internet facilities have been provided for official College/course related work: however personal use is permitted within the guidelines of this policy.

4.2 Intentionally accessing any material, which might be regarded as sexually explicit or offensive on the grounds of race, gender, disability, age, sexual orientation, religion or belief, pregnancy and maternity and gender-reassignment or which promotes extremist views is likely to be regarded as a disciplinary matter.

4.3 Intentionally accessing illegal websites is strictly forbidden and is likely to be regarded as a disciplinary matter. This will then be dealt with by the appropriate policies, procedures and if necessary, the relevant authorities (Police, ICO Commissioner)

4.4 Any user who accidentally visits sites mentioned in 4.2 or 4.3 (above) must leave the website immediately. Failure to do so may be interpreted as an intentional visit.

4.5 The internet connection has a finite capacity. Therefore users are encouraged not to download unnecessary large amounts of information, as this will degrade performance for others.

4.6 The downloading of MP3 or similar music or video files is strictly prohibited.

4.7 The College reserves the right to block what it considers to be unnecessary or inappropriate web sites and downloads. Students are encouraged to contact IT Support Team if they feel acceptable sites have been blocked.

4.8 The use of Internet Chat Sites or online games sites is prohibited on College computers and is likely to be regarded as a disciplinary matter.

4.9 Any attempts to disable, defeat or circumvent any of the College's computer security facilities (i.e. the use of proxy sites) is likely to be regarded as a disciplinary matter.

4.10 Whilst the College recognises students' right to a private life, during any use of social networking sites or maintenance of personal blogs (online diaries) students must remember that any personal information made available is within the public domain. Students are required to ensure that they do not write on the

sites in a way that could constitute the harassment of a student or employee of the College.

4.11 The College has software and systems in place to monitor and record all internet usage.

4.12 All electronic communication with Kingston Maurward College staff must only be via official KMC methods – your college email account, your course TEAMs group or Moodle. Under no circumstances should you communicate with your Course Manager or any other college staff via their personal social media accounts, their personal emails or their personal phones.

4.13 Videos used and stored by KMC on Moodle, including Plant eStream, must not be removed or copied, or subsequently uploaded onto any other media.

5 Email

5.1 The use of College computers to email jokes or material which might be regarded as sexually explicit or offensive on the grounds of race, gender, disability, age, sexual orientation, religion or belief, pregnancy and maternity and gender-reassignment or which promotes extremist views is likely to be regarded as a disciplinary matter.

5.2 No email communication which might be regarded as harassing or insulting may be sent using the College computers.

5.3 The facility to email all students must not be abused and should only be used for appropriate purposes and with the permission of a member of staff.

5.4 All users of the College's email systems are required to set up two factor multi authentication. Further guidance on how to do this can be found in the Bring Your Own Devices WiFi Connection Guides available on the Student Moodle Portal, or via the Learning Resource Centre Team or from the IT Support Team.

6 Security & Networks

6.1 No personal computer equipment may be connected to the KMC Network, either directly or remotely, without permission from IT Support Team. However, college Wi-Fi is provided for student use across the campus.

6.2 The College may use software to shut down PCs that are inactive for 15 minutes, therefore users must log off from the Network while away from the PC for more than 15 minutes in order to ensure that work is not lost, and that equipment is then made available for other users.

6.3 Passwords should be a minimum of 8 characters in length and include uppercase and lowercase characters, numbers and symbols. The use of "obvious" values such as people's names is discouraged.

6.4 Passwords must never be printed, stored or given out to anyone except members of the College IT Support Team – and only if required. If the IT Support Team need access to your account and you do not wish to give out your password then your password can be reset to allow access.

6.5 College Network drives have been allocated for the storing of College / course related work only.

6.6 The College will not be held responsible for the loss of any data from its network. Users are therefore reminded to keep separate back-up copies of all valuable work.

7 Bring Your Own Device (BYOD)

The BYOD Guides are located on the Student Moodle Portal; access to these documents is granted when you are enrolled with the College / UCKM.

7.1 Overview

Electronic Communication Device – such devices include laptops, notebooks, tablets, iPads, smartphones and any other devices that allow electronic communication.

Lost, stolen or damaged – Students who bring such devices into College do so entirely at their own risk, just like any other personal item.

Kingston Maurward College will not accept any responsibility for devices that are mis-placed, lost, stolen or damaged. Many devices have a location finder app and it is recommended that this feature is enabled to aid tracking.

It is also recommended that such devices are fully insured to cover loss and damage outside of the home. The College has lockers in many locations and these can be rented by students to place personal items when not required.

Security and Care – Students are responsible for the proper care and use of their own device.

Students are responsible for the adequate security of their own device whilst in College, keeping it with them when required or placed securely in a locker available for rent from the College. It is recommended that students do not share or lend their device to other students.

Educational use – Devices will only be used for educational purposes to support learning whilst in College. It will be at the teacher's discretion as to when these devices may be used by a student within lessons. Students will respect a teacher's decision and turn off their device when requested to do so.

Audio, Photographs and Video – Students will not use their device to record audio, or take photographs or video of other students and / or members of staff without their permission.

Students will not transfer or upload such media content without permission. Incidents of this nature, and where any form of harassment or upset occurs is likely to result in disciplinary action.

7.2 Connecting Devices to College Systems – connectivity of all mobile devices is centrally managed by the College IT Support Team, who must approve a device before it can be connected to the College systems.

The College reserves the right to refuse to remove permission for a student's device to be connected to the College systems. The College IT Support Team will refuse or revoke such permission where in their opinion a device is being or could be used in a way that puts, or could put, the College systems and data at risk or that may otherwise breach this policy.

In order to access the College systems, it may be necessary for IT Support Team to install software applications on the student's device. If the student removes any such software their access to College systems will be disabled.

7.3 Monitoring and Security Requirements – the College reserves the right to monitor, intercept, review and erase, without further notice, content on the devices connected to the College systems that is deemed to be in breach of this policy.

Monitoring, intercepting, reviewing or erasing of content will only be carried out in order to:

- Prevent misuse of the device;
- Ensure compliance with College rules, standards of conduct and policies in force

The College uses specialist software provided by Smoothwall which has the following functionality:

- Blocking illegal online content – Smoothwall is an Internet Watch Foundation (IWF) member and integrates the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.
- Inappropriate online content – Smoothwall will block access to sites covering a range of categories including extremism drugs, alcohol and pornography.

- Age appropriate differentiated filtering – Smoothwall is able to allow differentiated access to certain websites based upon approved criteria.

Students must comply with the College ICT Acceptable Use Policy when using their device to connect to the College systems.

The College reserves the right to inspect a student's device in order to ensure that it has not been used for unauthorised use. The student agrees to co-operate to enable inspection, access and review. Failure to co-operate may lead to access to College systems being removed.

7.4 Technical Support

The College cannot provide technical support for devices owned by students. If a student brings their own device to College, then they are responsible for any repairs, maintenance or replacement costs and services relating to this device.

8 General

8.1 Any user who is aware of any violations of this policy or any suspicion that unacceptable use has occurred should either report this to their Course Manager / Programme Lead or via a contact person as indicated in the Anti-Bullying and Harassment Policy.

8.2 The provisions in this policy apply to all ICT facilities including computers and computing facilities. Additional policies may be defined for specific equipment or locations.

8.3 This Policy may be modified from time to time, in response to changing circumstances, of an operational, legislative or technological nature.

8.4 Any person requiring clarification or further advice relating to this policy should, in the first instance, contact their Course Manager / Programme Lead.

8.5 The College reserves the right to use any evidence from emails, internet history or data stored on its networks or computers in any disciplinary or legal proceedings.

9 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 – there is the ability for these types of content to go viral.
- Phishing Attempts via Email – This is an attempt to pretend to be a company or person asking you to do something that results in gaining information from you – like your user name and passwords to key systems or apps that you use.

  Don't click on links or open documents in phishing attempts; it's the most common kind of attack.

  Be suspicious – if you have received an email asking you to do something, and you think there is something suspicious about it, report it to the IT Support Team immediately.

  Further information about personal fraud and scamming attempts can be found here: Dorset Police
- 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 on social media platforms 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 / Programme Lead 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 device or for access to their password details.